STRATEGY RESEARCH PROJECT

INTELLIGENCE SUPPORT TO HOMELAND SECURITY: SUPPORTING THE SUPPORTING EFFORT

BY

LIEUTENANT COLONEL PATRICK KELLY III
United States Army

USAWC CLASS OF 2002
Senior Service College Fellow

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INTELLIGENCE SUPPORT TO HOMELAND SECURITY: SUPPORTING THE SUPPORTING EFFORT

by

LTC Patrick Kelly III
United States Army

Colonel Michael Colpo
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Patrick Kelly III

TITLE: Intelligence Support to Homeland Security: Supporting the Supporting Effort

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 62 CLASSIFICATION: Unclassified

As the nation recovers from the shocking, tragic events of September 11, 2001, many talk openly about the operations that must follow. Intelligence operations are integral to the current and projected military operations, counter-terrorism operations, as well as the ongoing local, state, and federal crisis and consequence management of the terrorist attacks. Difficulties abound with collecting, processing, analyzing, and employing the intelligence required for these operations. Coordination of intelligence is a central component of the evolving responsibilities of the new Presidential Homeland Security Advisor. Implied is a restructuring of the intelligence community. An appreciation of the complexities surrounding future intelligence support to homeland security begins with defining homeland security and understanding basic intelligence functions. Juxtaposed against the attributes, roles, and responsibilities of intelligence, a framework of functions, architectures, and capabilities emerges.

The purpose of this paper is to provide a framework for understanding the complex requirements associated with intelligence support to homeland security. By examining capabilities and requirements, recommendations can be made for future restructuring of the intelligence community to meet the general and specific requirements of homeland security.

TABLE OF CONTENTS

PREFACE

Selection of the subject of this Strategic Research Paper (SRP) predates the terrorist attacks on September 11, 2001. During an August Consequence Management Symposium at Carlisle Barracks, sponsored by Frank Cilluffo (now at the Office of Homeland Security) from my fellowship host the Center for Strategic and International Studies (CSIS) and the Army War College Center for Strategic Leadership, I was informed of a future conference scheduled for March of 2002. The National Military Intelligence Association (NMIA) a professional organization of which I have been a member for many years had selected the topic "Intelligence Requirements of Homeland Security" for the National Intelligence Symposium 2002. I was intrigued by a potential SRP that combined my intelligence background, my recent Army Staff responsibilities for Homeland Security and Strategic Planning requirements. The events of September 11, 2001 only solidified my desire to completely examine a subject little understood suddenly receiving national and international attention.

Before commencing the Army War College fellowship at CSIS, I was assigned to Army War Plans (DAMO-SSW), newly moved into renovated Pentagon offices at 3C480. This office space no longer exists as it was directly in the path of American Airlines Flight 77. Miraculously, everyone in the office escaped. I am especially indebted to LTC Patrick Tennis, ARNG for his assistance in preparing this paper. LTC Patrick Tennis is a true American hero receiving a Soldiers Medal for his heroic rescue of trapped individuals in the Pentagon on September 11, 2001. I must also thank Dr. Jim Miller and LTG (Ret) Patrick Hughes, USA of the NMIA for allowing me to combine my research efforts with their excellent sponsorship of the aforementioned NMIA National Intelligence Symposium 2002. Finally, I must thank Dr. Kurt Campbell, Michèle Flournoy, and Dr. Philip Anderson of CSIS for their friendship and mentorship.

This paper is dedicated to the men and women who lost their lives on September 11, 2001; especially those of the Defense Intelligence Agency and Naval Intelligence who gave their lives at the Pentagon providing Intelligence Support to Homeland Security.

INTELLIGENCE SUPPORT TO HOMELAND SECURITY: SUPPORTING THE SUPPORTING EFFORT

> By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows: I hereby establish within the Executive Office of the President an Office of Homeland Security (the "Office") to be headed by the Assistant to the President for Homeland Security. The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.... The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States...
>
> Ensure that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies responsible for homeland security and, where appropriate for reasons of homeland security, promote exchange of such information with and among State and local governments and private entities.
>
> —George W. Bush

At his State of the Union address before Congress on 29 January 2002, President George W. Bush clearly articulated three national objectives for the nation, "To win the war [on terrorism], protect the homeland, and revitalize our economy." [1] The third national objective, economic security manifests itself in the weekly paychecks of the average American, the health of the economy, and the end of the current recession. The first national objective, victory in the war against global terrorism manifests itself in military victories, international coalitions, and the exercise of American global leadership. The second national objective, homeland security is more intangible. Homeland security requires psychological as well as a physical security. The absence of an attack on the United States does not prove the homeland is secure and may only represent a lull before a next more horrific attack. The role of the Intelligence Community is to support the federal government's attainment of all three strategic goals.

The global war on terrorism and homeland security can be perceived as two axis of a great campaign, a main and supporting attack. Both essential to ultimate victory, they co-exist and compete for scarce priorities such as the European and Pacific Theaters of World War II. One must be designated the main effort and the other is relegated to the supporting effort. Incorporating risk management, this designation allows prioritization of the scarce resources. One of the most important scarce resources is intelligence.

On October 8, 2001, President George W. Bush issued Executive Order 13228 establishing the Office of Homeland Security. The symbiotic relationship between homeland security and the global war on terrorism are immediately revealed in the functions of the office. "The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States." [2] Following a call for a National Strategy, the President outlined a series of specific intelligence responsibilities and functions.

> Detection. The Office shall identify priorities and coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism against the United States and activities of terrorists or terrorist groups within the United States. The Office also shall identify, in coordination with the Assistant to the President for National Security Affairs, priorities for collection of intelligence outside the United States regarding threats of terrorism within the United States.
>
> In performing these functions, the Office shall work with Federal, State, and local agencies, as appropriate, to:
>
> Facilitate collection from State and local governments and private entities of information pertaining to terrorist threats or activities within the United States;
>
> Coordinate and prioritize the requirements for foreign intelligence relating to terrorism within the United States of executive departments and agencies responsible for homeland security and provide these requirements and priorities to the Director of Central Intelligence and other agencies responsible collection of foreign intelligence;
>
> Coordinate efforts to ensure that all executive departments and agencies that have intelligence collection responsibilities have sufficient technological capabilities and resources to collect intelligence and data relating to terrorist activities or possible terrorist acts within the United States, working with the Assistant to the President for National Security Affairs, as appropriate;
>
> Coordinate development of monitoring protocols and equipment for use in detecting the release of biological, chemical, and radiological hazards; and
>
> Ensure that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies responsible for homeland security and, where appropriate for reasons of homeland security, promote exchange of such information with and among State and local governments and private entities.
>
> Executive departments and agencies shall, to the extent permitted by law, make available to the Office all information relating to terrorist threats and activities within the United States.[3]

This intelligence function framework highlights the Herculean requirements associated with intelligence support to both homeland security and the campaign against terrorism. The Office of Homeland Security homeland security framework of detect, prepare, prevent, protect, respond, and recover was heavily influenced by analysis previously performed by Analytical Services, Incorporated (ANSER). Establishing the vanguard for the debate on homeland defense and homeland security, in October 2000, ANSER created an Institute for Homeland Security and identified seven domestic missions: Deterrence, Prevention, Preemption, Crisis Management, Consequence Management, Attribution, and Response.[4] A myriad of Office of Homeland Security functional areas mirror the language of the Presidential executive order with the most relevant being the first "Detection, Surveillance, and Intelligence." A strong correlation between these homeland security frameworks establishes the requirements for intelligence support for homeland security.[5] In fact, the National Security Agency validated the framework through a series of workshops in the fall of 2001designed "to develop a framework to identify the actions required to achieve the stated and implied missions and tasks associated with the homeland security mission area."[6]

Even with Presidential direction and Intelligence Community attention, there still remains a great deal of uncertainty surrounding the homeland security missions and functions and the associated requirements for intelligence support to homeland security and the global war on terrorism. A National Security Strategy and National Homeland Security Strategy are under development. Definitions are absent for essential components beginning with homeland security itself. Even after assuming definitions and analyzing the Presidential directive to the Office of Homeland Security, there is an under appreciation for intelligence and its various manifestations and limitations. An intelligence functional framework highlights the extensive demands imposed upon the Intelligence Community to support both the main and supporting efforts of the dual campaign at home and abroad. Desperately needed for the Homeland Security framework is an operational architecture for the variety of systems and tools required for the counter-terrorism campaign and intelligence support to homeland security.[7] An analysis of the homeland security and intelligence functional frameworks eventually leads to recommendations for resource and organizational changes.

DEFINING HOMELAND SECURITY

Any appreciation of the role of intelligence relative to homeland security begins with definitional issues. An examination of intelligence definitions will follow shortly, but the discourse must begin with the many definitional issues associated with homeland security. The

current administration is heavily engaged in the development of a National Security Strategy. Absent this published document from the White House, we must extrapolate the homeland security role within the national security from published remarks of President Bush and his staff as well as a review of the source documents of the previous Clinton administration.

The President has spoken on numerous occasions since September 11, 2001 on the requirement to defend the homeland from terrorist attacks, most notably during his two addresses to Congress including his January 2002 State of the Union. Additionally, Executive Order 13228 signed on October 8, 2001 established the Office of Homeland Security. "The mission of the Office [of Homeland Security] shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." [8] Headed by Governor Ridge, this organization has the unenviable requirement to stand up authorities and procedures while simultaneously prosecuting a complex campaign. There is every expectation the National Security Strategy, expected in the summer of 2002, will generate a companion National Strategy for Homeland Security document. This strategy will join the National Military Strategy, the National Economic Strategy, and the National Foreign Policy Strategy in describing application of the elements of national power of the United States.

The requirements and strategy for homeland security did not materialize phoenix-like from the ashes of the World Trade Center and the Pentagon. For the last half dozen years numerous attempts wrestled with the issues of homeland defense and homeland security. The concepts codified in the National Security Strategy of 1996 were still discrete and described as Counterterrorism, Fighting Drug Trafficking and Other Missions. President Clinton introduced the requirements stating

> At the same time, the challenges to the security of our citizens, our borders and our democratic institutions from destructive forces such as terrorists and drug traffickers is greater today because of access to modern technology. Cooperation, both within our government and with other nations, is vital in combating these groups that traffic in organized violence. ... Countering terrorism effectively requires close, day-to-day coordination among Executive Branch agencies. [9]

By May 1997, the National Security Strategy outlined the requirements to protect against Transnational Threats that included Terrorism, Drug Trafficking, International Organized Crime, and Environmental and Security Concerns.

> Combating these dangers which range from terrorism, international crime, and trafficking in drugs and illegal arms, to environmental damage and intrusions in our critical information infrastructures requires far-reaching cooperation among the agencies of our government as well as with other nations. [10]

Throughout 1998 and 1999 homeland security requirements continued to be refined in the National Security Strategy. The maturation is clearly found in A National Security Strategy For A New Century of December 1999. In addition to a listing of transnational threats to the nation, the strategy clearly outlines components of the homeland defense. Although not quite a definition, these capabilities describe the requirements of homeland defense including: National Missile Defense, Countering Foreign Intelligence Collection, Domestic Preparedness Against Weapons of Mass Destruction, Critical Infrastructure Protection, and National Security Emergency Preparedness.

> Adversaries may be tempted to use long-range ballistic missiles or unconventional tools, such as WMD, financial destabilization, or information attacks, to threaten our citizens and critical national infrastructures at home. The United States will act to deter or prevent such attacks and, if attacks occur despite those efforts, will be prepared to defend against them, limit the damage they cause, and respond effectively against the perpetrators. At home, we will forge an effective partnership of Federal, state and local government agencies, industry and other private sector organizations. [11]

The culmination of the years of hard work and attention to the homeland security by the Clinton administration is their capstone strategy document A National Security Strategy for a Global Age published in December 2000.

> Emerging threats to our homeland by both state and non-state actors may be more likely in the future as our potential adversaries strike against vulnerable civilian targets in the United States to avoid direct confrontation with our military forces. Such acts represent a new dimension of asymmetric threats to our national security. Easier access to the critical technical expertise and technologies enables both state and non-state actors to harness increasingly destructive power with greater ease. In response to such threats, the United States has embarked on a comprehensive strategy to prevent, deter, disrupt, and when necessary, effectively respond to the myriad of threats to our homeland that we will face. [12]

Outlining seven mission areas associated with Protecting the Homeland, Combating Terrorism and Fighting Drug Trafficking & Other International Crime join the five previously outlined areas: National Missile Defense, Countering Foreign Intelligence Collection, Domestic Preparedness Against Weapons of Mass Destruction, Critical Infrastructure Protection, and National Security Emergency Preparedness. Even though not available on the White House homepage this document remains the published national security of the United States; in fact, it became obsolete and politically irrelevant even upon publication. The bitter Bush-Gore presidential election and the Bush repudiation of the Clinton engagement strategy of Shape, Respond, Prepare doomed this strategic document.

The Clinton Administration outlined a broad concept of homeland defense while debating the delineation of a detailed definition. The US Army initiated parallel planning and began an ongoing internal and external discussion of the roles, missions, responsibilities, and requirements of the Army for homeland defense. The first major contribution to the dialogue was the May 1999 U.S. Army Training and Doctrine Command (TRADOC) White Paper Supporting Homeland Defense. The doctrinal review of the homeland defense mission began with a postulated definition.

> Doctrine must refine and codify the definition of homeland defense consistent with practice, policy, and National Command Authorities' emphasis. Currently, the Department of Defense (DOD) provides no official definition of homeland defense; therefore, the following is proposed. Homeland defense is protecting our territory, population and critical infrastructure at home by: Deterring and defending against foreign and domestic threats; Supporting civil authorities for crisis and consequence management; and helping to ensure the availability, integrity, survivability, and adequacy of critical national assets. [13]

With the definitional framework established, the TRADOC white paper outlined broad categories or mission areas for the US Army. " The Army's role in homeland defense will fall into the following broad categories: force protection, support to crisis management, support to consequence management, protection of critical assets, support to counterterrorism, deterrence/defense against strategic attack, and MACA [Military Assistance to Civil Authorities] missions. Doctrine must expand, revise, or develop new guidelines to address each of these categories." [14] Although superceded in subsequent doctrinal and definitional discussions, the definition and categories shaped the homeland defense debate within the Department of Defense.

Always careful to defer to administration and departmental sensitivities about the evolving homeland defense mission areas, the Army continued its staff planning. The most obvious indicator of the political sensitivities associated with the undefined mission area was the migration of the concept from homeland defense to homeland security in the winter of 2000. In response to civil libertarian and bureaucratic concerns with the Department of Defense's role in the evolving mission areas, the Deputy Secretary of Defense John Hamre introduced the concept of homeland security. Since its introduction this concept has been used interchangeably with homeland defense without the necessary definitional clarity. On September 10, 2001, the Army published the coordinating draft of the Army Homeland Security (HLS) Strategic Planning Guidance.

> The purpose of this document is to promulgate strategic planning guidance for the Army to support an Army HLS assessment and the continuing development of the Army role, missions, and functions associated with HLS. The Strategic

> Planning Guidance is designed to define the scope of operations, identify critical operational nodes, and provide a baseline for implementing the necessary processes, programs and systems to ensure it is capable of effectively and efficiently supporting HLS requirements. [15]

Included within the strategic planning guidance is a revised homeland security definition modified from the original TRADOC homeland defense definition.

> Homeland security is those active and passive measures taken to protect the population, area, and infrastructure of the United States, its possessions, and territories by: Deterring, defending against, and mitigating the effects of threats, disasters, and attacks; Supporting civil authorities in crisis and consequence management; and Helping to ensure the availability, integrity, survivability, and adequacy of critical national assets.[16]

From this definition, the Army promulgated two broad mission areas and seven specific operations. Additionally the document outlined four tasks (deterrence, defense, crisis management, and consequence management) performed both before and after an incident.

> Homeland Security consists of two broad mission areas, *Homeland Defense* and *Domestic Support*, with distinct types of operations. This categorization is derived from the definition for HLS and a review of previously published policy, guidance and directives.
>
> ***Homeland Defense*** missions respond to the actions of a hostile or unwelcome force intruding on or attacking targets on U.S. sovereign territory. The missions associated with Homeland Defense include support to the following types of threats: Missile Attack; Air, Land, and/or Sea Sovereignty Incursion; Weapons of Mass Destruction Attack; and Cyber Attack.
>
> ***Domestic Support*** missions are conducted in reaction to or anticipation of a major disaster; act of civil disobedience, or to assist with a national-level event. The missions associated with domestic support include support to the following areas: Disasters; Civil Disorder; and Special Events.[17]

The influence of the TRADOC and Army doctrinal work is evident in the current Joint Staff and Office of the Secretary of Defense definitions of homeland security. In January 2002, the Joint Staff approved the following definitions:

> Homeland Security: The preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggressions directed towards US territory, sovereignty, domestic population, and infrastructure; as well as crisis management, consequence management, and other domestic civil support. Also called HLS. See also homeland defense and civil support.
>
> Homeland Defense: The protection of US territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also called HLD. See also homeland security and civil support.

> Civil Support: Department of Defense support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called CS. See also homeland security and homeland defense.[18]

The Department of Defense final codification of the four-year debate on Homeland Security definitions is not yet finished. The Office of the Secretary of Defense (OSD) is an active participant in the development of the National Security Strategy and responsible for the National Military Strategy that will codify the department position. Without these two documents the department's position must be inferred from other work. The Unified Command Plan (UCP) and the Quadrennial Defense Review (QDR) are two primary indicators of the department's commitment to homeland security. Also not yet completed and classified, the Unified Command Plan might not normally provide public insight into such a critical issue; however, this year's efforts clearly indicate homeland security activity. The department is publicly debating the creation of a tenth Unified Command, notionally called Northern Command or NORTHCOM. With geographic responsibility for North America, this command will potentially be responsible for all coordination of homeland security missions; especially the interagency process with federal, state, and local officials.

A less tumultuous indicator of the OSD position on homeland security is the QDR. Abandoning the Clinton strategy of engagement, Secretary Rumsfeld's defense department "developed a new strategic framework to defend the nation and secure a viable peace. This framework is built around four defense policy goals: Assuring allies and friends; Dissuading future military competition; Deterring threats and coercion against U.S. interests; and If deterrence fails, decisively defeating any adversary." [19] Focusing on Defending the United States and Projecting U.S. Military Power, the defense strategy clearly states, "Defending the Nation from attack is the foundation of strategy.... Therefore, the defense strategy restores the emphasis once placed on defending the United States and its land, sea, air, and space approaches. It is essential to safeguard the Nation's way of life, its political institutions, and the source of its capacity to project decisive military power overseas." [20]

A new force-sizing construct emphasized up front the forces necessary to Defend the United States placing "new emphasis on the unique operational demands associated with the defense of the United States and restores the defense of the United States as the department's primary mission." [21]

> The highest priority of the U.S. military is to defend the Nation from all enemies. The United States will maintain sufficient military forces to protect the U.S. domestic population, its territory, and its critical defense related infrastructure against attacks emanating from outside U.S. borders, as appropriate under U.S, law. U.S. forces will provide strategic deterrence and air and missile defense

> and uphold U.S. commitments under NORAD. In addition, DoD components have the responsibility, as specified in U.S. law, to support U.S. civil authorities as directed in managing the consequences of natural and man-made disasters and CBRNE-related [Chemical, Biological, Radiological, Nuclear, and Explosive] events on U.S. territory. Finally, the U.S. military will be prepared to respond in a decisive manner to acts of international terrorism committed on U.S. territory or the territory of an ally. [22]

Recognizing shortfalls, the QDR assessment continues:

> Ensuring the safety of America's citizens at home can only be achieved through effective cooperation among the many federal departments and agencies and state and local governments that have homeland security responsibilities. It is clear that the roles, missions, and responsibilities of the many organizations and agencies involved in national preparedness must be clearly delineated through an integrated interagency process. The Office of Homeland Security, which is responsible for overseeing and coordinating a comprehensive national strategy to safeguard the United States against terrorism and respond to any attacks that may come, will lead this important process. [23]

Concluding with the bureaucratic angst and the raw emotion of survivors of the Pentagon attack, the QDR paradigm shift embraces a next step not quite achieved by the Clinton national security team.

> It was clear from the diverse set of agencies involved in responding to the September 11, 2001 terror attacks on the World Trade Center and the Pentagon that the Department of Defense does not and cannot have the sole responsibility for homeland security. DoD must institutionalize definitions of homeland security, homeland defense, and civil support and address command relationships and responsibilities within the Defense Department. This will allow the Defense Department to identify and assign homeland security roles and missions as well as examine resource implications. DoD must be committed to working through an integrated inter-agency process, which in turn will provide the means to determine force requirements and necessary resources to meet our homeland security requirements. DoD must bolster its ability to work with the organizations involved in homeland security to prevent, protect against, and respond to threats to the territorial United States. In particular, the Defense Department will place new emphasis upon counter terrorism training across federal, state, and local first responders, drawing on the capabilities of the Reserve and National Guard. ... Integration of protection mechanisms (e.g., counterintelligence, security, infrastructure protection, and information assurance) will be a key component. In particular, the United States must enhance its capabilities to protect its critical infrastructure, especially infrastructure that supports oil and gas transportation and storage, information and communications, banking and finance, electrical power, transportation, water supply, emergency, and government services. [24]

The QDR Report of September 30, 2001 is one of the first Bush administration published official documents specifically addressing homeland security. Outlining a new defense strategy and anticipating a new national security strategy, this document was written, debated, and

revised prior to the events of September 11, 2001 with only a coda of acknowledgement that the future was upon us sooner than anticipated. In many ways the QDR assessment of homeland security is derived from the last published Clinton National Security Strategy. When correlated, six of the Clinton seven Protecting the Homeland mission areas are included in the QDR assessment. Only Fighting Drug Trafficking and Other International Crime, not specifically a defense department mission anyway, is missing from the priority homeland security missions. As witnessed during the first six months of the global war on terrorism, and in the President's January 2002 State of the Union message in which he said, "Stricter border enforcement will help combat illegal drugs;" [25] this mission area may yet also survive as a component of homeland security since it is so closely intertwined with combating terrorism.

As admitted by the QDR report, definitions are needed for homeland security. In fact, neither congress nor the executive branch has defined homeland security. Congressional deference to the executive branch's responsibilities is evident, though not absolute, throughout the debate on homeland security. Congress did take the opportunity to enter the debate through the National Homeland Security Act of 2001 (H.R.1158), sponsored by Representative Mack Thornberry (Republican-Texas) and the National Homeland Security Strategy Act of 2001 (H.R. 1292). This proposed bill, introduced in March 2001, sponsored by Representative Ike Skelton, D-Missouri "defines Homeland Security as, The protection of the territory, critical infrastructures, and citizens of the United States by Federal, State, and local government entities from threat or use of chemical, biological, radiological, nuclear, cyber or conventional weapons by military or other means." [26] This broadly scoped definition indicates Congress's central concern with weapons of mass destruction (WMD). "The scope of WMD in this proposed legislation is expanded with the addition of 'conventional weapons' and falls more in line with the title 18 of the United States Code definition of WMD and the acronym CBRNE. Also apparently excluded from this definition as a part of HLS is the element of natural disasters as defined in the Stafford Act and Title 10, USC." [27] Following the events of September 11, 2001, Congressional attention to the homeland security debate is manifested in a number of resolutions, task forces, and bills. Most germane to the issue of defining homeland security and intelligence support to homeland security are the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Public Law 107-56) and the Fiscal Year 2002 Intelligence Authorization Act (Public Law 107-108).

In response to the terrorist events of September 11,2001, as well as in response to the recommendations contained within bills like the Homeland Security Strategy Act of 2001 and

other influential commissions such as the Report of the United States Commission on National Security/21st Century (a.k.a Hart-Rudman Commission) and The Commission on Counter-Terrorism (a.k.a Gilmore Commision); President Bush created the Office of Homeland Security on October 8, 2001. Earlier in May 2001, responding to congressional and commission recommendations, the President designated the Vice President to lead the domestic preparedness effort as outlined in a statement "Domestic Preparedness Against Weapons of Mass Destruction." The events of September 11, 2001 greatly accelerated the administration focus on homeland security.

The President is committed to a clear articulation of a National Strategy for Homeland Security. It is the mission given to the Office of Homeland Security. Functions have been codified as "coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to and recover from terrorist attacks within the United States." [28] The timeline pronounced in the President's Homeland Security Policy and Budget Priorities statement "Securing the Homeland, Strengthening the Nation" is this year. Declaring Homeland Security "A New National Calling" the President commitment is steadfast:

> The higher priority we all now attach to homeland security has already begun to ripple through the land. The Government of the United States has no more important mission than fighting terrorism overseas and securing the homeland from future terrorist attacks. This effort will involve major new programs and significant reforms by the Federal government. But it will also involve new or expanded efforts by State and local governments, private industry, non-governmental organizations, and citizens. By working together we will make our homeland more secure. [29]

In his State of the Union speech, President Bush declares, "My budget nearly doubles funding for a sustained strategy of homeland security, focused on four key areas: bioterrorism, emergency response, airport and border security, and improved intelligence." [30] These four areas are an immediate budgetary focus; the President also promises, "The strategy will be comprehensive. It will encompass the full range of homeland security activities and will set priorities among them." [31] Here then is a presidential directive for a comprehensive, holistic strategy for Homeland Security promising challenges "of monumental scale and complexity" requiring a long-term; national, not just Federal; opportunistic; objective oriented; multi-year budgeted plan. [32] With the publication of the National Strategy for Homeland Security we will almost certainly obtain a definitive definition of Homeland Security. When published, it is almost certain that intelligence will remain integral to the strategy.

DEFINING INTELLIGENCE

Having failed to precisely define Homeland Security, an exploration of intelligence may yield better results. Like Homeland Security, there are no shortages of interpretation and definitions associated with Intelligence; however, there are a few definitive concepts that shape the discussion. From a defense perspective, intelligence is "the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas." [33] Yet, it should already be clear that homeland security intelligence is broader than this precise, holistic, yet narrowly focused definition. Additional varieties of intelligence: political, military, scientific and technical, economic, sociological, and environmental also are essential to homeland security intelligence. An alternative perspective is to explore the meanings of intelligence. The term intelligence is often interchangeably used to describe product, organization, mission, or process. Additional perspectives also describe intelligence cycles, disciplines, levels, and functions. All of these concepts and meanings are important when defining homeland security intelligence. [34]

INTELLIGENCE PRODUCT

The product of intelligence is information, or more precisely knowledge. The concepts of information, data, intelligence, and knowledge are often used without required precision. Data and information are raw materials which intelligence mines and manipulates to ascertain truths. However, intelligence must incorporate precision, accuracy, and timeliness in order to transcend into knowledge. Absent these characteristics intelligence reverts to history, trivia, or irrelevance. Intelligence is about knowledge, not secrets; that said, there is a great deal of secrecy surrounding the missions of intelligence organizations.

INTELLIGENCE ORGANIZATIONS

The Intelligence Community is the term used to describe those federal organizations involved in the collection and production of intelligence. This group is narrower than the larger group of intelligence consumers. The United States Intelligence Community consists of fourteen organizations. For years, the community had thirteen full members; however in the past two months the Untied States Coast Guard's contribution was recognized and they were elevated to a full partner in the community. The community can be easiest understood by dividing it into groups. The first group is the military service intelligence organizations. The Army, Air Force, Navy, Marine Corps, and now the Coast Guard each provide unique intelligence support for their respective services as well as provide a great deal of manpower for other agencies. The second group is the national intelligence agencies that support the entire

federal government, not just a discrete department. In addition to the Central Intelligence Agency (CIA), there are three organizations embedded within the Department of Defense (DoD) responsible to the larger community: National Security Agency (NSA), National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA). The final group is the departmental organizations. Starting with the Department of Defense, the Defense Intelligence Agency (DIA) supports the Department of Defense and the Joint Staff. Embedded within DIA are a variety of capabilities including the Central MASINT Office (CMO), the Defense HUMINT Service (DHS), and the Armed Forces Medical Intelligence Center (AFMIC). Every organization listed so far, with the exception of the CIA, belongs to the Department of Defense.

This organizational diversity demonstrates the senior partner status of DoD given its predominance of resources, both monetary and manpower. Whereas many will debate the role of the Department of Defense within the Homeland Security context, you cannot discuss intelligence support without describing the huge contribution of the DoD organizations, services, and agencies to the cause. The remaining Intelligence Community departments are the Department of Energy, the Department of Treasury, the State Department's Bureau of Intelligence and Research (INR), and the Department of Justice's Federal Bureau of Investigation (FBI) and Drug Enforcement Agency (DEA). Additionally the Department of Commerce and Department of Transportation maintain intelligence units essential to the Homeland Security mission. With the creation of the Transportation Security Administration (TSA) in November 2001 and the full inclusion of the Coast Guard into the Intelligence Community, it is highly likely the Department of Transportation will also soon achieve full membership in the Intelligence Community. [35]

The remainder of the Intelligence Community is the various boards, councils, and staffs. The National Foreign Intelligence Board (NFIB), the National Intelligence Council (NIC) and Community Management Staff (CMS) all assist the Director, Central Intelligence (DCI) to operate the diverse and complex intelligence apparatus. The President's Foreign Intelligence Advisory Board (PFIAB) and the Intelligence Oversight Board (IOB) provide executive oversight. The ultimate operational integration of course occurs at the National Security Council (NSC). For the moment the intelligence directorate of the Homeland Security Council is combined with the NSC under the supervision of the dual-hated GEN (Ret) Wayne Downing. Drawing upon the Second Gilmore Commission observation that foreign and domestic terrorism were no longer easily distinguished, a Heritage Foundation report recommends the creation of a Homeland Security Intelligence Coordinating Group (HSICG). This group would develop a

national intelligence strategy and establish resource and targeting priorities. [36] The already symbiotic relationship between the HSC and NSC reveals the potential redundant responsibilities of the future Homeland Security intelligence organizations and the existing national security intelligence organizations.

Perhaps, a better example of the potential bureaucratic flash points between homeland security intelligence and national security intelligence exists within the United States Congress. Congress as the legislative branch is excluded from the executive branch's Intelligence Community. Following extensive hearings in the 1970s most notably the Senate's Church Committee and the House of Representatives' Pike Committee, Congress recognized the overlapping jurisdictions associated with the intelligence community and created two select committees. First the Senate created the Senate Select Committee on Intelligence (SSCI) in 1976 and then a year later the House created the House Permanent Select Committee on Intelligence (HPSCI). In addition to providing a consolidated congressional oversight for intelligence activities for the past twenty-five years, these committees are often commended as prototypes for future homeland security select committees. Although future Senate and House Select Committees for Homeland Security would streamline congressional oversight, two of the potentially streamlined committees would include the HPSCI and SSCI. Since intelligence is critical to the homeland security mission area it is unclear how jurisdiction could be shared between these future four select committees and the myriad of other congressional committees.[37]

INTELLIGENCE MISSIONS

The simplest mission framework includes collection and analysis, counterintelligence, and covert action or special activities. It should come as no surprise that this framework corresponds to the internal organizations of intelligence units such as the Central Intelligence Agency. A more detailed discussion of intelligence collection follows shortly in the introduction of the intelligence disciplines, since collection is most usually associated with specific disciplines. The analytical mission requires a review of the intelligence cycle. The continuous, iterative process of intelligence is the essence of analysis. The phrase "sources and methods" is often appropriate when discussing the other two mission areas.

Counterintelligence is often described as an intelligence discipline when it is more accurately described as a mission since it uses a multi-disciplinary approach. The key to understanding counterintelligence is realization that the effort is focused upon the intelligence activities of an opponent. Historically this implied the foreign intelligence services of other

nations. With the rise of non-state actors and globalization, the framework is antiquated. Counterespionage is a narrower subset of counterintelligence focused on foreign spies. Counterintelligence is defined in Executive Order 12333 as "information gathered" and "activities conducted ... to protect against espionage, other intelligence activities, sabotage or assassination conducted on behalf of foreign powers, organizations or persons, or international terrorist activities ..." [38] Here then is clear authority for the counterintelligence mission of intelligence support to the counter-terrorism function of homeland security. The 2000 National Security Strategy includes Countering Foreign Intelligence Collection as one of the Protecting the Homeland mission areas stating, "We will continue to refine and enhance our counterintelligence capabilities as we enter the twenty-first century." [39]

Covert activity is the most titillating and therefore perhaps the least understood intelligence mission. Intelligence activities can be understood to be open, or overt, clandestine, or secretive, and covert, or plausibly deniable. In other words, "Covert action involves activities designed to influence foreign governments, events, organizations, or persons in support of U.S. foreign policy in such a way that the involvement of the U.S. government is not apparent." [40] The emphasis was on "foreign." Counterintelligence and domestic law enforcement employed similar capabilities; however, they were better described as sting, entrapment, or undercover operations. The focused emphasis on intelligence support to homeland security and the potential for abuses against U.S. persons and violations of constitutional protections makes this mission especially important.

Building upon a framework of the "escalation-ladder metaphor" designed by Herman Kahn, Loch Johnson offers an intriguing framework to explore the implications of covert actions on intelligence support to homeland security. Johnson outlines a "covert operations ladder of escalation" with thirty-eight options. These are codified within four thresholds: Routine Intelligence Operations, Modest Intrusions, High-Risk Operations, and Extreme Options. Passive security measures, observation, and sharing of low-level intelligence are examples of routine operations that are certainly appropriate for intelligence support to homeland security. The second tier involves recruitment of targets, technical surveillance, truthful propaganda, and low-level funding of groups. Although intrusive, these techniques are certainly consistent with existing law enforcement capabilities.

The third tier expands upon the modest intrusions and could frustrate domestic or international harmony if revealed. Truthful, but contentious propaganda, disinformation, high-level recruitment, more sophisticated technical surveillance, massive funding, economic, paramilitary, and ultimately military attacks clearly delineate a hierarchy of options potentially

available. Domestic, especially media, furor over the revelation of the Department of Defense's Office of Strategic Information's propaganda and disinformation support to the global war on terrorism demonstrate the sensitivities associated with employing these type activities. The final tier of especially dangerous and controversial extreme options range from theft, hostage taking, torture, environmental alterations, economic dislocations, coup d'etat, assassinations, secret wars, to using chemical, biological, or radiological agents. At first glance these appear too extreme for the homeland security mission area, yet with presidential authority, congressional oversight, and judicial review all have been employed previously. Following a protracted global war on terrorism and even more catastrophic or horrific attacks, there may yet be a shift in American psyche that would allow a gradual escalation along these lines, even against Americans. Presidents and their closest advisors engage in the policy, moral, and ethical debate surrounding these extreme covert options. [41]

INTELLIGENCE PROCESS

Intelligence missions, organizations, and products all rely upon an in depth appreciation of the intelligence process. Central to the intelligence process is the continuous, iterative intelligence cycle. There are five steps within the cycle: Planning and Direction, Collection and Processing, Analysis and Production, Dissemination, and Presentation.[42] Planning and Direction is normally the starting point within the iterative cycle. Intelligence requires a purpose. Requirements always exceed capability and therefore important prioritization decisions must start and end each trip around the cycle. Planning and Direction require continuous interaction with the customer to continuously refine requirements. The results of the planning effort are important prioritization for the available scarce resources. These prioritization decision are embedded throughout, but most often are reflected in the collection phase.

Collection involves the gathering of the raw data and information. Processing is the conversion of the raw data and information into an alternate format more easily analyzed such as language translation or telemetry conversion. Collection and processing are most normally associated with particular intelligence disciplines. These disciplines are Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signatures Intelligence (MASINT), Human Intelligence (HUMINT), and Open Source Intelligence (OSINT). As mentioned previously Counterintelligence (CI) is sometimes incorrectly listed as a unique discipline when it is in fact a multi-discipline approach to a specific mission. Technical Intelligence (TECHINT) is also sometimes considered a unique discipline but is another multi-discipline function focused on the scientific and technological developments of an opponent.

SIGINT results from collecting, locating, processing, analyzing, and reporting intercepted communications and non-communications emitters. SIGINT is often subdivided into communications intelligence (COMINT), electronic intelligence (ELINT), and Foreign instrumentation signals intelligence (FISINT). SIGINT is the responsibility of the National Security Agency. Since NSA is a national intelligence agency it supports all elements of the federal government including law enforcement allowing a seamless transition to intelligence support to homeland security. Always recognized as a preeminent technological organization, NSA is committed to an extensive transformation effort to preserve their preeminence. Through Herculean efforts, most notably the Unified Cryptologic Architecture, NSA is improving their capabilities to collect and process SIGINT. The advent of cellular, wireless, fiber optic, encryption, and Internet technology all present unique challenges for NSA and the Intelligence Community to maintain their premier SIGINT capability to support homeland security

Previously known as photographic intelligence, imagery intelligence is the product of imagery analysis. Imagery is derived from radar, infrared, optical, and electro-optical sensors. With technological advances new potentials exist for hyper-spectral and ultra-spectral imagery, blurring the distinction between IMINT and MASINT. The National Imagery and Mapping Agency (NIMA) is the premier though not exclusive imagery intelligence organization. Imagery analysis is undergoing transformation associated with digital capability. The newest director of NIMA, Lt Gen (Ret) Clapper outlines a concept of geospatial intelligence, "the analysis and visual representation of security-related activities on the Earth." [43] Imagery, or geospatial information is collected and processed by a variety of terrestrial, airborne, or satellite based collectors. The imagery community often redefines the intelligence process into front-end collectors and back-end processors. Essential to imagery collection efforts are the concepts of surveillance and reconnaissance. As typified by unmanned aerial vehicles (UAV), technological advances are allowing real-time continuous surveillance and stare of a target greatly enhancing intelligence and operational capabilities. The Orwellian Big Brother watching syndrome oft warned may in fact become a capability in the years to come as an intelligence tool to support homeland security

Least understood of the intelligence disciplines is MASINT. MASINT "uses information gathered by technical instruments such as radar's, lasers, passive electro-optical sensors, radiation detectors, seismic, and other sensors to measure objects or events to identify them by their signatures." [44] The ability to discretely tag a person, place, or thing due to unique signatures is an immensely valuable intelligence collection capability. MASINT is constantly

demonstrating important capabilities such as detecting weapons of mass destruction to finding hidden terrorists within caves.

Although all the intelligence disciplines are integrated into support for homeland security, HUMINT is the most critical. Often criticized for shortfalls in HUMINT capabilities, the Intelligence Community is committed to improving human intelligence collection. Recruitment of spies, operating agents, interrogation, and document exploitation are all examples of HUMINT collection. Often requiring extended preparation timelines; successful HUMINT collection is extremely lucrative. Tradecraft and language training are obvious investments in the resource intensive preparations necessary for human intelligence. As part of the post-September 11 backlashes additional resources are available, yet it will take years to recruit, train, and employ a new generation of human intelligence operatives. HUMINT is especially productive when combined with the other intelligence disciplines. "The intelligence disciplines must complement and cue each other for maximum effectiveness. Rarely will separate disciplines produce a comprehensive picture of the threat. Instead each discipline will produce bits and pieces of information which analysts will synthesize to approach a total picture." [45]

The final intelligence discipline is another under appreciated capability. Open Source Intelligence (OSINT) explores, exploits, and enhances generally available public information. Translations of the various international media are essential to monitoring situations. The Foreign Broadcast Information Service (FBIS) is the most recognizable of OSINT capabilities. In addition to written publications, radio, television, and the Internet are all monitored for relevant information. The OSINT methodology differs from other disciplines that focus on creating intelligence from scarce opportunities. OSINT must cull from an extraordinary volume of available information. Data mining and advanced search techniques are extremely important for OSINT. In this new environ, OSINT is far more important than ever before.

There are two critical components of the analysis and production step analytical methodology and tools. All too often well-intentioned recommendations focus upon the tools supporting the analysts without an appreciation for the underlying analytical methodologies. Almost all analysis can be summarized within fundamental logic of inductive or deductive reasoning. Inferring patterns and assembling disparate pieces into a coherent whole are essential to the current pattern based intelligence analysis. In response to the current and anticipated asymmetric threats a newer pattern less analytical methodology is receiving increased attention, which will be applicable to the homeland security problem set. The importance of analytical tools will be examined in greater detail in a subsequent discourse.

The flip side of collecting and processing data and information is the dissemination of the resultant intelligence. Sources and methods is the community shorthand to protect the ability to exploit enemy weaknesses. The post analytic product derives its classification from these sources and methods. Classification levels, caveats, sanitization, and handling instructions are all important considerations that will be further examined in the horizontal and vertical dissemination of homeland security intelligence and the resultant requirement for multi-level security. The most important consideration for dissemination is speed not security. Intelligence is often perishable and the dissemination system must be robust enough to guarantee immediate delivery.

Closely related to dissemination is the final step in the intelligence process, presentation. Decision makers ranging from tactical commanders or first responders to senior policy makers and executives all differently assimilate intelligence and knowledge. Intelligence must be tailored to the needs of the decision maker. Modern technology and weapons require digital interface. Short succinct presentation, whether oral, visual, or written are all required at various times. Failure to properly present intelligence can negate all previous intelligence endeavors.

Interchangeably using intelligence to describe product, organization, mission, or process demonstrates the complexity of intelligence support in general. Mixing in confusion about the intelligence cycle, disciplines, levels, and functions further complicates an understanding of intelligence support to homeland security.

HOMELAND SECURITY INTELLIGENCE FUNCTIONS

As the nation recovers from the shocking tragic events of September 11, 2001, many talk openly about the follow-on operations. Intelligence operations are integral to any projected military options, counter-terrorism operations, as well as the ongoing crisis and consequence management of the terrorists attacks themselves. Difficulties abound with collecting, processing, analyzing, and employing the intelligence required for these operations. An appreciation of the complexities surrounding future intelligence options must begin with the basic intelligence functions. Examining the role of the six basic intelligence functions against the demands of a homeland security and counter-terrorism campaign provides a framework to begin addressing much more complicated strategic and policy issues.

The six intelligence functions are: Indications & Warning, Intelligence Preparation, Situation Development, Target Development, Damage Assessment, and Force Protection. The iterative interaction of these fundamental intelligence requirements highlights the immensity of the undertaking. Each of the intelligence disciplines must support all six functions. Larger

policy issues associated with coalition operations, operational security, and abridging or the inevitable impact upon civil liberties begin with these six functions.

INDICATIONS & WARNING

The numerous post-mortems of the terrorist hijacking attacks appear split almost evenly on the question of a strategic intelligence failure. In outrage and frustration many ask how such a complex operation could go undetected. Historical queries and a complete reexamination of available evidence will almost certainly identify potentially enlightening intelligence.[46] In effect, the perceived intelligence failure represents a failure of the Indications and Warning (I&W) function. Others recognize the secretive, conspiratorial nature of these crimes and concede, even if indicators were recognized, is warning really possible for such a heinous suicidal event? The indications and warning function cannot limit itself to post-mortem self-flagellations. The terrorist network constitutes a dedicated, thinking, adaptive opponent who must also prosecute additional events if their campaign is to succeed. After the fact analysis will reveal investigative and prosecutorial leads which the intelligence community will support. However, warning of the next attack, as well as responding to the anticipated false positives resultant from heightened awareness, could consume the resources and talents of all available intelligence and law enforcement professionals. While awaiting the next strike can be perceived as reactive, the intelligence operations associated with indications and warning are in fact some of the most proactive. Long-term human intelligence operations, extensive counter-intelligence operations, and sophisticated monitoring are aimed at providing the notification, but more importantly the warning of the next attack. Supporting any extensive collection operations are the skillful application of the analytic prowess of the intelligence community's thousands of analysts.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

The analytic component of intelligence operations is must often associated with the intelligence preparation of the battlefield (IPB) function. Traditional military intelligence IPB concentrates on weather, enemy, and terrain. Expansion of the essential preparation function quickly includes social, economic, and political requirements that cannot be overlooked, but are for the moment saved for the situation development function. Inherent within the preparation function is enormous data management requirements. Narrow discussions that focus on data, data retrieval, metadata, information technology, and data management identify the science of intelligence without an appreciation for the art. Knowledge is different from intelligence, which is also different from information. Terrorism is a worldwide phenomenon, the opponents' campaign plan exploits this to simultaneously hide in plain site and squirrel away into the darkest holes evil

can find. The information associated with an active dynamic world is the wheat field from which single grains must be threshed and culled to successfully find and fight terrorists.

Returning briefly to the more traditional IPB military requirements highlight some terrain and weather challenges the intelligence system must address. Associating the Taliban regime in Afghanistan with these crimes highlights the extreme terrain that can drastically impact military operations. The extended area of operations for the terrorist network around the world reveals another geographic component of intelligence operations, wide area surveillance. Contrary to the predications of dime store novelists, there are limitations to the reconnaissance and surveillance capabilities available to the US intelligence community. Most are rooted in programmatic shortfalls and the laws of physics that is best understood by the inability of any single limited resource of being in two places simultaneously. Well documented in the ongoing Quadrennial Defense Review is the shortage of command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) assets. The collection requirements for homeland security and counter-terrorism operations, albeit at the highest priority, will still compete alongside all other requirements. Identifying the terrain, providing images of this terrain, populating the digital databases of sophisticated systems with the appropriate geo-spatial information are all essential for the terrain component of the IPB function. Everyone knows the intelligence officer's bane - an intelligence report begins with the weather. Second only to intelligence failures associated with I&W, weather confounds the intelligence system. The intelligence system is responsible for the failures of weather to cooperate. Blessed with state of the art satellites and extraordinary computer simulations, weather prediction is phenomenal. Unfortunately, correct forecasts for remote mountainous or desert terrain do not negate the impact of weather extremes on military operations that may require prosecution in these regions.

The essence of preparation resides in the ability of the combined talents of the intelligence community analyst to employ inductive, deductive, predictive, and sometimes just lucky analysis that reduces complex thought and behavior into something simple and comprehensible. No detail is too mundane, no understanding complete. Bridging the functional requirements between indications and warning and situation and target development, intelligence analysis attempts to learn and understand all applicable background information. The modern terrorist is at home in the technological world; as low tech as the jet fueled suicide bomb might appear, an appreciation for structural engineering, avionics, and communications demonstrates increasing technological sophistication. The preparation function must catalogue and analyze worldwide financial transactions and state of the art computer and communications networks, as well as

history, heritage, and culture. Counter-terrorism relies upon the expertise of the special operations community, which successfully integrates these complex requirements into an IPB template.

SITUATION DEVELOPMENT

Yet a template is not enough. The thinking, adaptive terrorist is constantly changing with the situation. The Situation Development function integrates all the capabilities of the intelligence system to the problem at hand. Constantly guarding against the mirror-imaging phenomenon, situation development is the interaction of the U.S. capabilities with the antagonistic and elusive terrorist. Many will talk about perfect intelligence or 90% certainty about an operation. The intelligence professional attempts 99% certainty on the 1% event potentially consuming everyone's attention. Certainty after the fact is history, certainty too early or disclosed before the fact allows the terrorist to alter their strategy or course of action. Knowing what needs knowing without extraneous information is the requirement the operational community places upon the intelligence community. That said, commanders and operators immerse themselves in the details of intelligence to assist their operational assessments. Stated another way, every operation is preceded by an intelligence operation. These operations range from the infantryman walking point on patrol or the reconnaissance unmanned aircraft providing real time images to complex human intelligence and counterintelligence operations years in the making. The Bush administration's calculus of a protracted campaign against terrorism recognizes that numerous intelligence operations will not appear overnight. Establishing networks of foreign agents, analyzing communication and computer networks, financial forensics, and developing psychological, cultural, religious, and political templates are all intelligence operations within the protracted campaign against the terrorist.

TARGET DEVELOPMENT

Given the already pervasive retaliatory rhetoric and the grave repercussions to any significant mistake, the Target Development function will receive extraordinary scrutiny throughout the campaign. Images of precision munitions flying through specifically targeted windows morph when two decades of fighting already rubble the building or the location is a mountain cave. Target development must be broadened to include financial networks that law enforcement experts can attack, information and propaganda operations attempting to manipulate local and world opinion, and terrorist cells that operate in isolated secrecy. Target development will have greater success against supporting infrastructure, but identifying the infrastructure supporting a terrorist cell or network and preventing collateral damage against

innocents will require patience as well as precision. One dilemma always present but exacerbated in this situation is the balance between disclosing information and the sources and methods used to derive it. The great difficulty penetrating potential terrorist cells, the time sensitive nature of targeting intelligence, and a desire and requirement to protect sources and methods may conflict. Imagine a human intelligence operation months or years in the making that becomes a one time operation because the source is isolated, compromised, killed as a result of targeting actions; the intelligence system is not robust enough in some areas of the world to treat every intelligence operation as a one time mission. Innovations in the field of measurements and signatures intelligence (MASINT) may assist in tracking and targeting terrorists in remote areas of the world, but may also be limited by the close-in access required for some systems. Cyber-targeting against the sophisticated cosmopolitan terrorist is also problematic. Aside from the encryption dilemma which complicates collection operations, the more difficult issue is direction finding. In the days of old, radio and radar signatures could be geo-located on the battlefield. On the modern battlefield, the systems are designed to preclude locating the emitters, but more importantly how is an Internet service provider operating on the global information system (GIS) geo-located in time to prosecute targetable intelligence. The difficulties associated with these requirements should not be underestimated. And, of course, sources and methods once again come into play as intelligence operatives attempt to protect lucrative sources while military and political operatives seek tangible exploitation of the derived intelligence and demonstrable destruction and defeat when achievable.

DAMAGE ASSESSMENT

Even as the difficulties associated with target development are reconciled, the next intelligence function may be the hardest of all. Assessment, or battle damage, of counter-terrorist operations is so counter-intuitive as to become paradoxical and produce paranoia. In effect, since successful counter-terrorist operations cause nothing to occur, how does the intelligence system assess the success of nothing? Simplistically, they return to I&W functions and monitor indicators. However, proactive counter-terrorist operations endanger innocents as well as eliminate terrorists and their operations. Propaganda and information operations are sure to trumpet every failed counter-terrorist attempt even as military operators strictly enforce operational security. The non-linear battlefield upon which we must engage the modern terrorist does not lend itself to quantifiable lines on an operational map as in the Second World War or even the body count methodology so blasphemed in Vietnam. Dual use is another dilemma that hampers assessment. The Internet site operating as a terrorist front or the school trained pilot

becoming a suicidal bomber are examples of dual use blurring of the boundary seam exploited by the terrorist. Assessing prior performance is important, but more important is anticipating the next heinous pattern-less twist the determined terrorist imparts. Measures of effectiveness are difficult to ascertain and even more difficult to populate once established. The intelligence system must accomplish this Herculean task while executing the other five functions.

FORCE PROTECTION

The final intelligence function is Force Protection. Integrating with the other five functions, intelligence support to force protection relies upon counter-intelligence, active and passive force protection measures, and operational security to minimize friendly vulnerabilities while simultaneously exploiting enemy vulnerabilities. The continuous iterative interaction of the determined terrorist opponent requires constant vigilance. Vulnerability assessments require expertise that the intelligence system must provide. Deception and espionage must be anticipated and negated. Communications security and information security are integrated within a comprehensive operational security plan. Physical barriers and mental alertness discourage incidental attacks causing the determined terrorist opponent to seek ever more creative sensational attacks. Barriers and alertness degrade over time and complacency may return, combining with the I&W function, force protection support must compensate and contribute, especially after attention spans shift to future activities. This counter-terrorist endeavor by design will involve a coalition further complicating intelligence support to force protection. In Bosnia, the Stabilization Force operates at least six different classification levels as information is shared differently with coalition partners. These necessary provisions protect sources and methods as well as comply with American and coalition partner laws.

The requirements of any one of the intelligence functions will place grave demands upon the intelligence system as it supports homeland security and the counter-terrorism campaign. In combination the requirements increase exponentially. One nuance that may be lost is that intelligence capabilities are supplemental not incremental. The intelligence system must exploit all known vulnerabilities even while exploring and exploiting new vulnerabilities. The fog of war associated with military operations often requires operating in a degraded mode. Often one operation is designed to cause the opponent to revert to procedures that can be exploited. The terrorist is not constrained by timelines and willingly hides for extended periods of time. The intelligence system scans the world while focusing with laser precision for discrete periods of time upon an individual, an organization, or a location. This requires capabilities and resources often husbanded and concentrated. The old adage is intelligence is never held in reserve. A

protracted campaign places astronomical demands upon intelligence, exposing system shortfalls. Organizational inefficiencies, programmatic and bureaucratic competition, and perceived shortfalls will all receive intense scrutiny. Information age thirst for constant information will challenge even secrecy itself. The intelligence professionals prosecuting the near term campaign in response to the terrorist attack are capable of great success. Most often these successes derive from the immense dedication and talents of the men and women of the intelligence profession.

HOMELAND SECURITY INTELLIGENCE TOOLS - VOICES

In his budgetary statement on "Using 21st Century Technology to Defend the Homeland", President George W. Bush addresses intelligence tools and information technology.

> The President's budget calls for an increase of $722 million and sets in motion a program to use information technology to more effectively share information and intelligence, both horizontally (among Federal agencies and Departments) and vertically (among the Federal, State and local governments). This ongoing homeland security initiative is a key component of the President's "Expanded Electronic Government" management initiative for the entire Federal government, which seeks to improve the way that agencies work together to serve citizens by maximizing the benefits of the Federal government's overall investment in information technology.[47]

The initiative outlines two key objectives: "Goal 1 - Tear down unwarranted information 'stovepipes' within the Federal government and Goal 2- Share homeland security information with States, localities, and relevant private sector entities."[48] The complex intelligence functions supporting homeland security require premier analytic tools. Tremendous tools abound throughout the intelligence community. Application of these tools requires an operational architecture framework to emphasize the homeland security intelligence requirements. A proposed framework is articulated by the acronym VOICES. The Virtual Operational Intelligence Collaborative Environment – Secure (VOICES) outlines the interaction and integration of the various tools required to support homeland security. [49]

VIRTUAL

The virtual world expands exponentially as the entertainment, education, and financial communities apply the latest in telecommunications and computational technologies. The intelligence community chases the vanguard in many of these virtual endeavors. The integration of live, simulated, and virtual worlds is essential to the intelligence support to homeland security and the prosecution of a global war on terrorism. Only in a virtual world can the complexities of real-time intelligence feeds, analytical simulations, and predictive scenarios

combine to anticipate and prevent catastrophic events. The current campaign in Afghanistan reveals the awesome potential for real-time unmanned aerial vehicle (UAV) surveillance. Whether Global Hawk or Predator, the ability of current generation UAVs to provide instantaneous images for reconnaissance, surveillance, and target acquisition will only improve with new tactics, techniques and procedures. Integrating live intelligence from the various disciplines with complex simulations is also essential, especially when modeling the effects of weapons of mass destruction. The ability to integrate and present the intelligence and knowledge gained from the current and next generation of SIGINT and MASINT sensors also requires extraordinary computational prowess. Presentation of the intelligence will take place in a virtual world as templates, modeling runs, and live data are seamlessly exchanged into a common operating environment. Finally, the intelligence support for the cyber dimension of the threat as well as the tools for force protection exist and are best understood in a virtual context. For years, the intelligence community has been accused of living in a closed, secretive world isolated behind the proverbial green door. In order to provide intelligence support for homeland security and the global war on terrorism the green door opens into a virtual world.

OPERATIONAL

To say that homeland security requires an operational framework appears overly simplistic. Yet the integration of the various operations within homeland security and the global war on terrorism is extremely complex and necessitates operational oversight. As demonstrated in the initial post-mortem of the events of September 11 2001, no detail is too insignificant as an indicator. Intelligence support for the military, political, diplomatic, legal, economic, and informational elements of national power requires increased integration. All six intelligence functions, especially indications and warning, force protection, and target development require intelligence operations. Intelligence operations precede, support, and post-mortem every operation. Reducing uncertainty will never be absolute always placing stresses upon the intelligence system. Difficult prioritization decisions will always be required. Characterization of main and supporting efforts within and across the elements of national power will delineate prioritization for scarce intelligence resources. Risk associated with less intelligence for supporting efforts requires increased emphasis on efficient intelligence operations to release full potential. Demands for new tools and system upgrades most often will occur online as an organization, capability, or technology will require almost immediate application to the homeland security and war effort. Operational application of best practices

and new technologies will place great stress on an already taxed operational intelligence system.

INTELLIGENCE

The entire intelligence community supports homeland security. All the intelligence disciplines possess unique as well as common tools. The National Security Agency exploits the mathematics of encryption, wave theory, and computation to collect, process, and analyze the ever-changing signals environment. Human intelligence organizations rely on psychology, cultural, and motivational tools to gain understanding and exploitation of sources, agents, and adversaries. The document exploitation and interrogation on the battlefields of Afghanistan employ both high technology and century old techniques. All six intelligence functions are embedded throughout the prosecution of the campaign. The iterative intelligence cycle never wanes. Integration, appreciation, and optimization are noble goals that require continuous attention to the tools of the trade.

COLLABORATIVE

Collaboration is one of the least appreciated aspects of intelligence support to homeland security. There is an obvious integration and collaborative spirit within and across the homeland security intelligence community. This is best understood through an examination of the current premier intelligence tool Intelink. "The '*Intelink* Community' is quite large and spans a broad spectrum of users since it consists of both intelligence 'producers' and intelligence 'user' organizations. Indeed, the *Intelink* Community is considered by many to be the 'ultimate information producers' in terms of volume, number of users, and mission: to support efforts to ensure and maintain the security of this nation."[50] In addition to the collaborative spirit, there are also constantly improving collaborative tools. These tools rely upon innovations in computation and telecommunications and are known as collaborative computing.

A National Security Agency research scientist, Robert Ferrone, defines collaborative computing as,

> Providing geographically dispersed networked computer users the simultaneous capability for audio, full action videoconferencing, whiteboarding, and document and applications sharing on a real time basis, almost as if they were in the same room together... Real-time collaborative computing will encompass simultaneous group and desktop videoconferencing, applications sharing, sharing of computer screens, and meeting management, all in a seamless environment among two or more people. [51]

Email is of course the most common of these tools. Extrapolating from this definition, "we define the ultimate in collaboration to be the *ability to electronically see, hear, and interact with a geographically disconnected person or group of people as though they were not separated.*[original italics]" [52] Full appreciation and exploitation of the current and next generation of collaborative tools will change the tactics, techniques, and procedures of intelligence support to homeland security.

Even as the intelligence community wraps itself in the chrysalis of collaborative community tools, the homeland security intelligence community metamorphoses. The federal family involved in homeland security and their associated intelligence organizations continue to emerge from the cocoon. Leading the change is of course, the Homeland Security Office led by Tom Ridge. On March 19, 2002, President Bush signed Executive Order 13260 Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security,

> I hereby establish the President's Homeland Security Advisory Council (PHSAC)... The appointed members of the PHSAC shall be selected from the private sector, academia, professional service associations, federally funded research and development centers, nongovernmental organizations, State and local governments, and other appropriate professions and communities.[53]

The relationship between the PHSAC and existing intelligence oversight organizations such as the President's Foreign Intelligence Advisory Body (PFIAB) and the Intelligence Oversight Board (IOB) as well as operational entities such as the National Foreign Intelligence Board (NFIB) and the Community Management Staff (CMS) and ultimately the entire intelligence community will require careful constructs.

It is certain that a strong working relationship between the Homeland Security Office and the National Security Council (NSC) will continue. In fact, the current director of the homeland security office intelligence portfollio is dual hatted with responsibilities for the NSC as well. In December 2001, the Homeland Security expanded from the White House to create a national coordination center that is designed "to break down technological and bureaucratic barriers that block information sharing among agencies like the C.I.A. and F.B.I."[54] Collaborative bureaucratic reorganization also underlines fundamental constitutional issues as witnessed by the month long stalemate between the United States Senate and the White House on Director Ridge's refusal to testify before Congress.

Another collaborative uncertainty is the Department of Defense reorganization in response to the homeland security mission. No final decisions have been made, but it is anticipated that the Department will stand up a new Unified Command, notionally called Northern Command,

and a new Under Secretary for Homeland Security to provide appropriate civilian control for the evolving mission areas. Regardless of final decision the new command will possess some form of Joint Intelligence Center or JIC and some type of command and control center. Drawing upon exisiting available tools as well as designing new tools, the intelligence support to homeland security will be enriched by the computational, collaborative, and data-mining advanced information technology employed by the new command.

ENVIRONMENT

Never forgetting it is the people and not the tools that make the ultimate difference, the ideal environment is a combination of push and pull technologies as well as the employment of both intranets and extranets that will allow intelligence support to homeland security to operate. One recommendation from a recent Heritage Foundation report Defending the Homeland called for "improving intelligence and information sharing among all levels of government with homeland security responsibilities," with specific steps including "creation of a federal-level fusion center" and a "structure for sharing and disseminating information among Federal, State, and Local agencies." [55] Recognizing the negative environment currently existing for information and intelligence sharing, the White House reported current spending at $155 million with $722 million more requested in next year's White House budget proposal. "Under a directive issued by President Bush, and overseen by Office of Homeland Security officials, CIA and FBI officials are 'working like crazy' to create a comprehensive database that could be used by various federal and, in some cases, state agencies." [56]

These efforts and others to come are relying on anticipated improvements in data mining. This can be accomplished through advanced computational innovations and better search engines, but ultimately rests with the data itself. One of the most important improvement to data management is the use of metadata. "The term metadata is often defined in various information systems glossaries as 'data about data' or 'data which relate to other data.' Metadata refers to machine-readable document 'tags' or other data that provide descriptions for collections of distributed information." [57] Better data management through required, if applicable, and optional tags as well as standards such as the World Wide Web's Hypertext Markup Language (html) are the essential nuts and bolts of making metadata retrieval faster and more relevant. Improving the flow of intelligence support to homeland security will require improved flow of data through push and pull technology. In the world of intelligence push technology allows the distribution of information, best understood in the pre-internet world as message traffic. Pull

technology allows the rapid retrieval and or selective data mining of someone else's files and or intelligence. A balance of these technologies is essential to the proper environment.

The media where the flow and exchange of intelligence occurs is the intranet or extranet. "The term extranet is a recent buzzword that really describes a special type of intranet. While *intranets* are internal systems designed to connect users within a specific 'community of interest' (such as *Intelink* in the case of the U.S. Intelligence Community), *extranets* are extended intranets that connect to outside customers and other more strategic partners." [58] There are many lessons learned from the formation of INTELINK that are directly relevant to the formation of a homeland security intelligence environment. In addition to the previously discussed metadata standards, there are also security and access control applications. The environment must implement need to know security, encryption, personnel and physical security, and both physical and virtual access control.

SECURE

The employment of multilevel information systems security introduces the final aspect of the tool suite. The dictionary definition of security is "the state or feeling of being free from fear, care, danger." When discussing intelligence and networks, security is "protecting information from unintended access." [59] Central to the use of multilevel security is the concept of certificate authority. Just as metadata provides data on data, certificates provide data on users. "Through the application of public key cryptography, the Certificate Authority (CA) provides a centralized mechanism by which certificates can be issued to all of the users as well as the individual servers out on the network. It is through these certificates that secure, encrypted, channels can be established and easily administered on the network." [60] Security Management Infrastructure (SMI) employs strong authentication, end-to-end confidentiality, enhanced access control, and network auditing and monitoring. The tools of SMI include encryption (key management), certificate management, and communities of interest. [61] Disparate communities of interest make intelligence support to homeland security different.

There are currently multiple instances of the intelligence network Intelink. There are four basic families of users separated by classification levels: Intelink-Special Compartmented Information (Intelink-SCI), Intelink-SecretNet (Intelink-S), Intelink-PolicyNet (Intelink-P), and Intelink-UnclassifiedNet (Intelink-U) and a special intranet connecting the United States, the United Kingdom, Canada, and Australia Intelink-Commonwealth (Intelink-C). Homeland security intelligence currently employs all of these networks. "Not only do the different instantiations of Intelink make communication among their users relatively difficult, they also

make management of the available information relatively more difficult." [62] "Intelink has *multiple security levels* rather than *multilevel security*." [63]

Missing from these multiple security levels is the connectivity to state and local officials and the private sector. It is the connectivity to the various private participants essential to homeland security that makes the potential Intelink – HomelandNet (Intelink-H) exponentially more complicated. Private partnerships are essential for the push and pull flow of information in fields such as energy, telecommunications, medical, and transportation. The federal family is a national family. It is the connectivity and access of private citizens and corporations that makes multilevel security unlikely without major technological breakthroughs. Multilevel security is the ideal, which must shape the creation of the various tools. "The key characteristic of such an approach would be a single, unified network shared by all Intelink users. To provide secure access control under this scenario, only communication from a higher classification level to a lower one would be allowable, while the opposite direction would not be permitted." [64] As long as multiple levels of security continue, isolation and duplication will complicate intelligence support to homeland security.

The Virtual Operational Intelligence Collaborative Environment – Secure (VOICES) provides a framework for the expansion of the tool suite necessary for meeting the President's challenge of using 21st century technology to defend the homeland. Innovations and technological breakthroughs will improve the tools. Organizational and bureaucratic restructure will allow talented individuals to design and implement such a framework. The world will not remain static as the intelligence community develops and implements the necessary tools. University, industry, and federal frustration with the limitations of the Internet has already resulted in the creation of Internet2 "a faster, smarter, more capable Internet, one that puts the needs of science and education first." [65] The homeland security VOICES network will exploit the next generation virtual partnerships, remote control, distance education, and virtual databases associated with Internet2 and subsequent Internet innovations. While the potential for technological innovation appears promising, especially given the increased funding flowing toward homeland security intelligence function, ultimately it is the intelligence professionals that will make the system work. Any increased monetary resources must fund premier quality, quantity, expertise, and training of tool operators, not just the tools.

IMPLEMENTING AND IMPROVING INTELLIGENCE SUPPORT TO HOMELAND SECURITY

Intelligence operations are central to the campaign against terrorism. Beginning with the post mortem debate on the intelligence failure of September 11, 2001 and probably culminating

in a redesigned intelligence community, America is focused upon intelligence with a laser-like intensity. A prism is perhaps the more appropriate metaphor for considering the intelligence community and intelligence operations supporting the counter-terrorism campaign. Examining the various intelligence responsibilities reveals a fractured rainbow of organizations not always seamlessly combined into a coherent whole. Distinctions among disciplines and intelligence roles must blur in order to tear down artificial walls to allow better cooperation within and across the intelligence community. In addition to the potential reforms there are well-documented deficiencies within the intelligence system, most notably inadequate human intelligence capability. Time, as well as resources, is necessary to address many deficiencies that will require patience from political leaders, the American public, and coalition partners. An adjunct to intelligence operations is direct action activities associated with covert communities and special operations that play an extremely active role in a counter-terrorism campaign. Even while improving intelligence capability, the nation must remain alert to the possible infringement upon civil liberties of all Americans in order to successfully prosecute the counter-terrorist campaign and secure the American homeland.

Although the nature of the counter-terrorism campaign is touted as new and different, this is not true for the intelligence system. Both publicly and, more importantly, privately the intelligence community has been actively involved in counter-terrorist operations. Examining the role of the six basic intelligence functions against the demands of a counter-terrorism campaign provides a framework to begin addressing much more complicated strategic and policy issues. The six intelligence functions iteratively interact highlighting the immensity of the undertaking. Juxtaposition against the overarching goals and notional objectives of the campaign reveals the magnitude of the intelligence requirements and highlights shortfalls in capability that must be addressed.

Since the intelligence community was firmly committed to the counter-terrorism campaign prior to September 11th, support to a first strategic goal *Sustain the firmness of American purpose both at home and abroad* involves sustaining the commitment. Cooperation within the intelligence community and maximizing opportunities for intelligence sharing with coalition partners are concrete manifestations of the commitment. The intelligence functions of situation and target development are essential to tracking and targeting the terrorists, their networks, and the nation states that harbor them. A second strategic goal *Define global terrorism and lead the campaign to outlaw it* highlights the intelligence preparation and assessment functions. A third strategic goal *Build stronger counter-terrorism capabilities across the board, but particularly for homeland security* reinforces the situation and target development functions while also

highlighting the force protection function. Defending the American homeland is the ultimate force the intelligence system must protect throughout the campaign. A final strategic goal *Develop a new strategy and declaratory policy for deterring, retaliating and preempting terrorist and the states that harbor or support them* includes all the previous functions and restates the importance of a robust indications and warning intelligence function to deny the terrorist all safe haven and preclude future catastrophic events.[66]

SOURCES AND METHODS

As the world becomes more aware of the intelligence operations required to support a protracted campaign against terrorism, many will, for the first time, become aware of the complex world of intelligence. Secrecy, uncertainty, and complexity are commonplace but little understood outside a small faction of informed insiders. The community shorthand for intelligence collection and analysis is sources and methods. Protecting sources and methods is intuitively important. However, twenty first century communications and the global information system conspire to expose the very fundamental sources and methods upon which intelligence operations depend. The healthy tension between protecting sources and methods and the requirement to provide timely warning and potential prosecution of terrorism transgressors will dominate the debate surrounding the current and protracted campaign against terrorism.

In ever increasing operations, human intelligence is required to access technical capabilities. The symbiotic interaction of human intelligence and the more technical disciplines is the essence of intelligence sources. The tactics, techniques, and procedures employed by both technical and human intelligence capabilities determine the methods of intelligence collection. Redundancy is designed into an operation to compensate for uncertainty and to eliminate single points of failure. Diligent counterintelligence capabilities constantly assess current vulnerabilities and aspire to disrupting ongoing intelligence operations of a determined opponent. In the high stakes world of sophisticated technical and human intelligence operations, mere knowledge of specific intelligence is enough to compromise a lucrative source, since the information can be traced back to a finite location, time, or group of individuals.

The ability to prosecute a successful campaign against terrorism will require all the talents and innovations of the current intelligence community. Biologic concepts such as gestation, germination, and incubation accurately describe the nurturing, extended time-lines, and fragile nature associated with translating a surge of resources to intelligence professionals and intelligence operations into meaningful intelligence. Although all aspire to immediate contribution and utmost effort is ever-present, intelligence professionals like professional athletes require

coaching and seasoning before all-star caliber performance is achieved. Once pinnacle performance is achieved, it is even more difficult to sustain. Combinations of specialists and generalists are essential to maintain a superior intelligence community. Computer proficiency, analytical prowess, linguistic propensity, keen intellect, and patriotic fervor are all welcomed; however, these aptitudes must coalesce into a coherent operative or analyst and then be integrated into ongoing capabilities.

Money thrown against technical shortfalls will almost certainly produce results, but not necessarily in the immediate future. The National Security Agency is in the midst of retooling its capabilities for the twenty first century. The Director has been vocal in educating the nation of the challenges and the costs associated with addressing these concerns. The information revolution components of encryption, digitization, fiber optics, and computer technology are not new challenges for the nation's cryptographic and signals intelligence communities. What is new is the integration of some of these technologies and the increased emphasis on access, a de facto return to old procedures, the integration of technical and human intelligence operations.

The siren song that the United States long neglected human intelligence resonates across land. However, the short-term infusion of resources must address systematic shortfalls as well as hire the next generation of intelligence operatives. An appreciation of human intelligence's contribution begins with an understanding of agents and networks. The primary purpose of an intelligence agent is to establish and maintain a network of sources. The rejection rate on acquiring access through the recruitment of credible sources is extremely high. The preparation alone is measured in weeks and months, if not years. In many ways, the willing source may be the most suspect. It appears restrictions imposed upon the intelligence community recruitment of less honorable persons are dissipating, but a system of checks and balances will still be maintained to ensure control of disreputable sources as well as return on investment.

A final component of the sources and methods discussion is a requirement for investment in technologies. Just as the intelligence system must invest in the personnel, there must also be an investment in the technical tools of the trade. Improvements in miniaturization, communications, computational capability, power generation, stealth, and signature are all ongoing. Continued investment in technologies and the operational application of technologies will ensure the intelligence professionals develop the next generation of capabilities to maintain America's advantage.

The current intelligence community emerged during the Cold War; and therefore, post Cold War reorganization is essential. Recognition of the continuous nature of the electromagnetic spectrum requires restructuring of agencies dedicated to a particular

bureaucratic interpretation. Education of traditional field operatives with ever changing technical capabilities is also essential. The intelligence community and law enforcement communities can surge for extended periods of time and the numerous task forces are testament to the flexible nature and fusion potential of current organizations. However, the system cannot sustain high tempo operations for the period of a protracted campaign. The intelligence agencies and organizations require new operators and analysts and an exponential increase in manpower to ensure redundant coverage of high value, lucrative, fleeting targets.

ANALYSIS

There has always been a healthy tension between the field operators and collectors who generate intelligence and the thousands of analysts who process the material. America's reliance on technical collection capabilities created a generation of analytical experts who master the intricacies of a particular intelligence discipline such as photographic or signals intelligence. The mosaic created from the integration of all available sources of intelligence is robust and less susceptible to deception.

Although a dearth of precise intelligence is always a possibility, the converse is a more accurate depiction of the intelligence system. The intelligence community is awash in information. Images, communications, and human reports swamp the system on a daily basis. Analysts cull through the information and through inductive and deductive reasoning develop intelligence. A structured collection management system prioritizes scarce resources and cross-cue other collectors and analysts of fleeing opportunities. Many mistake advances in computational capability as analysis. The computer and the associated databases are the tools that the analysts exploit. The housekeeping of the computer systems competes for the analysts' scarce time best spent thinking and analyzing. Retraining for new systems and capabilities can actually degrade an organization's capability.

Prosecuting a protracted campaign against terrorist networks with global reach requires analytical expertise of many disciplines. Although many generalists are scattered throughout the intelligence community, specialists, not always interchangeable, are required. Financial forensics received a great deal of media focus as suspected terrorist funds were frozen. Beginning with basic accounting and economic skills, the financial pathologist acquires banking and computer skills usually specializing in an organization or a region. Gaps in collection coverage are articulated to the collection management system that iteratively seeks new collection opportunities. As vital as these skills are to the counter-terrorist campaign, these individuals are already in great demand and are not interchangeable with the analyst attempting

to infiltrate and record the activities of a terrorist cell. These individuals require linguistic, cultural, and political skills. The intersection of the terrorist and his banker do not necessarily result in a corresponding intersection of the equivalent analysts.

One of the major shortfalls of the analytic community is a propensity to mirror image, or expect an adversary to behave the same way we would. The psyche revealed by suicidal bombers does not lend itself to immediate comprehension. The intelligence community anticipates future terrorist events seeking an escalation of sensationalism, political significance, and possibly casualties. This possibility draws the intelligence community into the high-risk world of weapons of mass effects. The consideration of weapons of mass destruction: nuclear, biological, chemical, or radiological weapons add yet another dimension to the expertise required by the intelligence community. The intelligence support to the world of counter-proliferation associated with maintaining control of these catastrophic weapons is a sub-discipline unto itself often requiring years of schooling and practical experience.

COMMUNITY OF COMMUNITIES

Although the initial advantage is with the terrorist, the intelligence community must negate the asymmetrical advantage and seize the initiative. The United States and its coalition partners will address the terrorist organizations with the application of the all elements of national power. The intelligence system must support each element to its own advantage. The most visible will be the reconnaissance support to any military operation. Behind the scene are the thousands of analysts and the thousands more required for the protracted campaign. One of the most lucrative sources of intelligence for the United States will be the contribution of coalition partners. Sharing of intelligence among nations is commonplace. With an ever-present eye on sources and methods this sharing must increase and quicken to match the pace of an agile, thinking opponent.

Developing the intelligence coalition to support the terrorist campaign may prove to be simultaneously the easiest and most difficult component of the campaign. Many of the pledges of support from around the world will never see the light of day because the support will manifest itself in the sharing of intelligence. In this context, intelligence shared with coalition partners must be considered as a perishable commodity. Operational security concerns are magnified when coalition partners are involved. The coalition partners, especially Arab and Islamic nations will provide the United States access and context otherwise not readily available or very time consuming to generate unilaterally. Coalition partners will not want their investment in lucrative sources or intelligence operations compromised by the United States any more than

we would welcome compromise of our sources and operations. Therefore intelligence will be shared with caveats and procedures to minimize, but never eliminate, the risk of compromising sources and methods.

As the coalition matures, multilevel security will become a regular requirement. Operations may be planned without direct or only limited access to the underlying intelligence and analysis. The easiest multilevel arrangement is bilateral where two nations agree to share specific intelligence. Sharing among multiple nations will almost certainly require establishing procedures such as those used by NATO nations or the coalitions in the Balkans. In order to change the behavior of individuals or nations, or perhaps re-establish sovereignty following decisive military operations, non-governmental organizations and private volunteer organizations may become involved in future phases of the counter-terrorist campaign. Although sharing intelligence is not likely, sharing of information is possible. Also, media from around the world can be expected to cover the campaign and investigative journalism may potentially undermine or reveal intelligence sharing among nations.

The military roles within the campaign will be limited by the contribution of law enforcement, economic, information, diplomatic, and political elements of national power. Each of these capabilities has intelligence organizations, albeit none as large as the Department of Defense. These varied agencies and capabilities constitute the interagency intelligence community. Fusion within the community is essential. Bureaucratic and programmatic fiefdoms must yield to the common cause. Unfortunately, with an initial inclination to throw resources at the campaign, underlying inefficiencies may be masked in the short and mid-term. The bureaucratic barriers will breakdown with nothing short of a new National Security Act within the next couple of years.

Fusion implies sharing information. Fusion also implies timely dissemination of both raw information and finished intelligence. The fleeting targets within a counter-terrorist campaign will require accurate, timely dissemination of indications, warnings, and targets. For example, once a new airport security and Sky Marshal system are operational, how will specific intelligence be disseminated to the constantly moving marshals? Although the deterrent value cannot be underestimated, a proactive component of the program must arm them with intelligence not just revolvers. Numerous proposals will attempt to marry perishable intelligence with a new system and may become a de facto new intelligence bureaucracy, such as recent proposals to create an expanded Border Security Agency.

Underlying all concerns about intelligence operations with interagency and coalition partners is the concern for operational security. The very nature of counter-terrorism operations

places them among the most secretive of government operations. The expectation of informed governance and media monitoring of the proposed protracted campaign place many operations at risk of exposure, failure, or compromise. The American population and media appear willing in the short term to allow the intelligence and special operation communities to begin prosecution of direct action and covert operations of the campaign. Sustaining the support will require a concerted flow of information to the population and the fourth estate. This information cannot be allowed to jeopardize ongoing and projected intelligence operations. Aside from the sources and methods and coalition sensitivities previously discussed, there is the risk of failure that must be considered. The small groups and individuals sought in a worldwide counter-terrorism campaign are elusive from the start. Operational security and terrorist cell tactics severely limit opportunities to obtain targetable intelligence. Even post-mortem examination of failed missions can compromise potential operations and must be avoided.

Essential to the successful campaign is a robust counter-intelligence capability. The counter-intelligence discipline employs all of the other components of the intelligence system to provide a multi-discipline examination of potential terrorist operations. Counter-intelligence operations, within America purview of the Federal Bureau of Investigation, are aimed at disrupting the intelligence apparatus of the terrorists. Before the fact, these activities provide the indications and warning essential to severely undermine terrorist activities. After the fact, they provide the framework for collecting evidence for law enforcement prosecution. The techniques of counter-intelligence and law enforcement are very similar. The blurring of the legal distinctions between these functions requires great scrutiny in order to protect American civil liberties. Legal precedent is well established for suspension of privacy rights in certain circumstances such as criminal investigations against suspects or counter-intelligence investigations. General blanket application of capabilities such as electronic surveillance or search and seizure is not likely to occur; however, redefinition of responsibilities and loosening of procedures will occur in order to secure the homeland. Many of the current laws regarding collection against foreign enemies are dated by cold-war rhetoric. Globalization and the information revolution require updating of the procedures without compromising the underlying constitutional rights.

RECOMMENDATIONS

An appreciation for the complexity of the intelligence operations supporting the counter-terrorism campaign reveals some shortfalls that require attention in order to provide intelligence support to the main and supporting efforts. The global war on terrorism and homeland security

are inexplicably intertwined; however at any given moment one must be the main effort and the other de facto becomes the supporting effort. Symbiosis is anticipated and expected, but requirements always exceed resources. Commitment of resources alone, although welcomed, will not solve some issues. Coordination and cooperation will address many systematic issues. Recommendations to more efficiently prosecute the intelligence support to homeland security and the counter-terrorism campaign include:

- Continued commitment to unifying the efforts of the intelligence community manifested in processes to enhance collaboration and information sharing.
- Increase of resources and personnel for human intelligence operations.
- Focus on analysis through investment in a generation of intelligence analysts.
- Investment in intelligence system research and development.
- Adoption of a Homeland Security operational architecture incorporating the VOICES framework.
- Increase of counter-intelligence resources and capabilities.
- Expansion of the counter-proliferation intelligence infrastructure.
- Continued emphasis on fusion of interagency and coalition intelligence.

Publication of President Bush's National Security Strategy and a Homeland Security Strategy in the summer of 2002 will most likely address many of the highlighted shortfalls. Parallel efforts such as the ongoing Lt Gen (Ret) Scowcroft- led review of the Intelligence Community will also most likely address other relevant issues.[67] The events of 11 September 2001 appear to many as a watershed and a wakeup call. For the intelligence community they were neither. Diligent pursuit of terrorist organizations preceded and certainly post-dates the tragic incidents. Commitment to the task never waned. Prioritization of scarce resources sometimes hindered successful counter-terrorist operations. In the wake of the terrorist attacks, the intelligence community is receiving additional resources and will undergo reflection and probable reorganization. More importantly, the intelligence system will bring to bear all the talents of the intelligence community to the task of intelligence support to homeland security.

WORD COUNT = 15,438

ENDNOTES

[1] George W. Bush, "The President's State of the Union Address, " (Washington, D.C.: The United States Capitol, 29 January 2002). The text of the President's State of the Union Speech is located at <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html>.

[2] George W. Bush, Executive Order 13228 Establishing Office of Homeland Security and the Homeland Security Council (Washington, D.C.: The White House, October 8, 2001), 1.

[3] Ibid.

[4] Ruth A. David, "Why is Homeland Security so Difficult?," Analytic Services Inc, (ANSER) briefing Slides presented to the Center for Strategic and International Studies, Washington, D.C., ANSER, 21 December 2001.

[5] Ibid. The complete list of functional areas as expressed by the Homeland Security Council Policy Coordination Committees are: Detection, Surveillance, and Intelligence; Plans, Training, Exercises, and Evaluation; Law Enforcement and Investigation; Weapons of Mass Destruction (WMD) Consequence Management; Key Asset, Border, Territorial Waters, and Airspace Security; Domestic Transportation Security; Research and Development; Medical and Public Health Preparedness; Domestic Threat Response and Incident Management; Economic Consequences; and Public Affairs.

[6] Patricia M. Newman and James Player, Homeland Security: Report on the Workshops to Define a Framework for Action (Fort George G. Meade, MD: National Security Agency, January 2002), 1. The results of the Homeland Security workshop facilitated by ANSER and attended by representatives from over thirty organizations will be used by the National Security Agency to develop thinking, plans, and activities for its role in homeland security.

[7] Also required are system and technical architectures which are appreciated, but well beyond the expertise of the author.

[8] George W. Bush, Executive Order 13228 Establishing Office of Homeland Security. 1.

[9] William J. Clinton, A National Security Strategy of Engagement and Enlargement (Washington, D.C.: The White House, February 1996), 19-20. The Federation of American Scientists homepage historical archive provided the electronic copy of the 1996 National Security Strategy located at <http://www.fas.org/spp/military/docops/national/1996stra.htm>.

[10] William J. Clinton, A National Security Strategy for A New Century (Washington, D.C.: The White House, May 1997), 13. The National Archives and Records Administration version of the Clinton White House homepage provided the electronic copy of the 1997 National Security Strategy located at <http://clinton2.nara.gov/WH/EOP/NSC/Strategy/>.

[11] William J. Clinton, A National Security Strategy for A New Century (Washington, D.C.: The White House, December 1999), 16. The National Archives and Records Administration version of the Clinton White House homepage provides an electronic copy of the 1999 National Security Strategy at <http://Clinton4.nara.gov/media/pdf/nssr-1229.pdf>.

[12] William J. Clinton, A National Security Strategy for a Global Age (Washington, D.C.: The White House, December 2000), 20.

[13] Department of the Army, U.S. Army Training and Doctrine Command (TRADOC), Supporting Homeland Defense, White Paper (Norfolk, Virginia: U. S. Department of the Army, May 1999), 1.

[14] Ibid., 4.

[15] Department of the Army, Army Homeland Security (HLS) Strategic Planning Guidance, (Washington, D.C.: Department of the Army, 10 September 2001), 1-2.

[16] Ibid., 6.

[17] Ibid.

[18] Department of the Army, "JCS Approved HLS Definitions," briefing slide from the Army G-8 Deputy Chief of Staff for Programs, Washington, D.C., Headquarters Department of the Army, 14 February 2002.

[19] Department of Defense, Quadrennial Defense Review Report, (Washington, D.C.: Department of Defense, 30 September 2001), 11.

[20] Ibid., 14.

[21] Ibid., 17.

[22] Ibid., 18.

[23] Ibid.

[24] Ibid. 19-20.

[25] George W. Bush, State of the Union Address.

[26] Department of the Army, Army HLS Strategic Planning Guidance, 9.

[27] Ibid.

[28] Bush, Executive Order 13228, 1.

[29] George W. Bush, Securing the Homeland, Strengthening the Nation (Washington, D.C.: The White House, February 2002), 3. The President's Homeland Security Policy and Budget Priorities statement is located at <http://www.whitehouse.gov/homeland/homeland_security_book.html>.

[30] Bush, State of the Union Address.

[31] Bush, Securing the Homeland, Strengthening the Nation, 6.

[32] Ibid. The criteria listed are taken from the President's highlighted plan for a National Strategy for Homeland Security. The complete list is found on pages 6-7.

[33] Joint Chiefs of Staff, U.S. Department of Defense Dictionary of Military Terms (New York: Arco Publishing, 1988), 183.

[34] Loch K. Johnson, Secret Agencies: U.S. Intelligence in a Hostile World, (New Haven: Yale University Press, 1996), 2-13. Loch Johnson's framework was one of the most succinct and applicable explanations of the various concepts of intelligence. Also very helpful was Jeffrey T. Richelson's The U.S. Intelligence Community. Either book well establishes the framework for understanding intelligence before exploring the various nuances.

[35] Jeffrey T. Richelson, The U.S. Intelligence Community, 4th ed. (Boulder, Colorado: Westview Press, 1999), 12. The definitive unclassified accounting of the U.S. Intelligence community is Richelson's book.

[36] Daniel W. Fisk, "Top Priorities for Improving Intelligence and Law Enforcement Capabilities," A Report of the Working Group on Intelligence and Law Enforcement in the Heritage Foundation report Defending the American Homeland (Washington, D.C.: Heritage Foundation, 2002), 58.

[37] Johnson, 89. Johnson's chapter 4 gives an extremely readable accounting of the Congressional turmoil associated with standing up the intelligence oversight committees.

[38] Richelson, 332.

[39] William J. Clinton, A National Security Strategy for a Global Age, 22.

[40] Richelson, 349.

[41] Johnson, 60-69. I am indebted to Loch Johnson for the framework and the rethinking of intelligence and covert action escalation found in chapter 3.

[42] Department of the Army, Intelligence and Electronic Warfare Operations, Field Manual 34-1 (Washington, D.C.: U.S. Department of the Army, 27 September 1994), available from <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-1/toc.htm>; Internet; accessed 6 April 2002. and Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations, Joint Pub 2-0 (Washington, D.C.: Joint Chiefs of Staff, 9 March 2000), available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf>; Internet; accessed 6 April 2002. The author uses a six-step intelligence cycle found based on FM 34-1 and Joint Pub 2. The Joint framework outlines five steps: planning and direction, collection, processing, production, and dissemination. It is the absence of the clear delineation of the presentation step in the joint cycle that caused me to modify the framework.

[43] National Imagery and Mapping Agency (NIMA), NIMA Statement of Strategic Intent, (Washington, D.C.: National Imagery and Mapping Agency), iii.

[44] Department of the Army, Intelligence and Electronic Warfare Operations.

[45] Ibid.

[46] Even as this paper was reaching final review, the debate continued. House and Senate intelligence committees are planning hearings to investigate the intelligence failure associated with September 11, 2001. Steve Hirsch, "CIA performance disputed as Congress plans hearings," Government Executive Magazine, 1 April 2002, <http://www.govexec.com/news/index.cfm?mode=report&articleid=22605>; Internet; accessed 6 April 2002.

[47] George W. Bush, "Using 21st Century Technology to Defend the Homeland," available from <http://www.whitehouse.gov/homeland/21st-technology.html>, Internet, accessed 6 April 2002.

[48] Ibid.

[49] The acronym VOICES is based upon some work I did in 1997 for the Deputy Chief of Staff for Intelligence while assigned to the Army Intelligence Master Plan (AIMP). An early version of the concept VOICE was used by LTG Kennedy in a briefing at INSCOM and by the Intelligence and Electronic Warfare Division of the Force Development Directorate of the Deputy Chief of Staff for Plans and Operations (DAMO-FDI) in a briefing to the Vice Chief of Staff of the United States Army. These two briefings are the only instances of which I am aware that the framework was used previously.

[50] Fredrick Thomas Martin, Top Secret Intranet: How the U.S. Intelligence Built INTELINK – The World's Largest, Most Secure Network, Charles F. Goldman Series on Open Information Management (Upper Saddle River, New Jersey: Prentice Hall, PTR, 1999), 25.

[51] Ibid., 178.

[52] Ibid., 179.

[53] George W. Bush, Executive Order 13260 Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security (Washington, D.C.: The White House, March 19, 2002), 1.

[54] Alison Mitchell, "Ridge Is Opening a Center to Analyze Data," New York Times, 25 December 2001, The New York Times on the Web available at <http://www.nytimes.com/2001/12/25/national/25RIDG.html>; Internet; accessed 3 April 2002.

[55] Daniel W. Fisk, "Top Priorities for Improving Intelligence and Law Enforcement Capabilities," A Report of the Working Group on Intelligence and Law Enforcement in the Heritage Foundation report Defending the American Homeland (Washington, D.C.: Heritage Foundation, 2002), 62.

[56] Greg Seigle, "CIA, FBI developing intelligence supercomputer," Government Executive Magazine 12 February 2002; available at

<http://www.govexec.com/news/index.cfm?mode=report&articleid=22264>; Internet; accessed 3 April 2002.

[57] Martin, 207.

[58] Ibid., 25.

[59] Ibid., 90-91.

[60] Ibid., 128.

[61] Ibid., 127.

[62] Ibid., 149.

[63] Ibid., 150.

[64] Ibid.

[65] Brad Lemley, "Internet 2: A Supercharged New Network with True Tele-Presence Puts the Needs of Science First," Discover, May 2002, 64.

[66] Clark Murdock, "Nature of the Campaign and Overarching Objectives," unpublished Version 3 of Chapter 3 "The Imperative to Prevail and the Nature of the Campaign" in the Center for Strategic and International Studies collaborative effort To Prevail: An American Strategy for the Campaign Against Terrorism, (n.p.), October 2001. Clark Murdock's outstanding four strategic goals framework for the campaign against terrorism fell victim to the editing process and is absent from the final version of To Prevail.

[67] Walter Pincus, "Rumsfeld Casts Doubt On Intelligence Reform Changes Suggested by Presidential Panel," Washington Post, 9 April 2002, sec. 1A, p. 17. Lt Gen (Ret) Brent Scowcroft, chairman of the President's Foreign Intelligence Advisory Board (PFIAB), is currently leading a Presidential-directed extensive review of the Intelligence Community. The National Security Council reportedly reviewed preliminary results in late March. Any analysis of this effort is premature, but must include a review of the National Security Act. Possible reorganization of the Intelligence Community and Congressional consideration of multiple proposals to create a Homeland Security Agency could all culminate in a new National Security Act.

BIBLIOGRAPHY

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. First Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. I. Assessing the Threat. James S. Gilmore III, Chairman. 15 December 1999. Available from <http://www.rand.org/nsrd/terrpanel/terror.pdf>. Internet. Accessed 9 April 2002.

____. Second Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction II. Toward a National Strategy for Combating Terrorism. James S. Gilmore III, Chairman. 15 December 2000. Available from <http://www.rand.org/nsrd/terrpanel/terror2.pdf>. Internet. Accessed 9 April 2002.

____. Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: III. For Ray Downey. James S. Gilmore III, Chairman. 15 December 2001. Accessed 9 April 2002. <http://www.rand.org/nsrd/terrpanel/terror3.pdf>.

Agüera, Martin and Douglas Barrie. "Allies Remain Reluctant to Share Intelligence." Defense News, 1-7 October 2001, 4.

Anderson, Philip. "Critical Infrastructure Protection Series." Symposium Moderator. Session One: Telecommunications; Session Two: Public Health. Washington, D.C., Center for Strategic and International Studies, February 2002.

Andrew, Christopher M. For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush. New York: Harper Collins, 1995.

Bamford, James. Body of Secrets: Anatomy of the Ultra-Secret National Security Agency – From the Cold War Through the Dawn of a New Century. New York: Doubleday, 2001.

____. The Puzzle Palace. Boston: Houghton Mifflin, 1984.

Betts, Richard K. "Fixing Intelligence." Foreign Affairs 81 (January /February 2002): 43-59.

Brinkerhoff, John R. "The Relationship of Warning and Response in Homeland Security." Journal of Homeland Security. October 2000. Available from <http://www.homelanddefense.org/journal/articles/displayArticle.asp?article=27>. Internet. Accessed 6 April 2002.

Bush, George W. "The President's State of the Union Address. " Washington, D.C.: The United States Capitol, 29 January 2002. The text of the President's State of the Union Speech is located at <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html>.

____. Executive Order 13260 Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security. Washington, D.C.: The White House, March 19, 2002. The Executive Order is located at <http://www.whitehouse.gov/news/releases/2002/03/20020321-9.html>.

_____. Executive Order 13228 Establishing Office of Homeland Security and the Homeland Security Council. Washington, D.C.: The White House, October 8, 2001. The Executive Order is located at <http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html>.

_____. Homeland Security Office Home Page. Available from <http://www.whitehouse.gov/homeland/> .Internet. Accessed 5 April 2002. A comprehensive catalogue of the Bush Presidency Homeland Security efforts. A catalogue of all homeland security presidential and director activities and statements is available from <http://www.whitehouse.gov/homeland/archive/html>.

_____. Homeland Security Presidential Directive-1(HSPD-1) Organization and Operation of the Homeland Security Council. Washington, D.C.: The White House, 29 October 2001. HSPD-1 is located at <http://www.whitehouse.gov/news/releases/2001/10/20011030-1.html>.

_____. Securing the Homeland, Strengthening the Nation. Washington, D.C.: The White House, February 2002. The President's Homeland Security Policy and Budget Priorities statement is located at <http://www.whitehouse.gov/homeland/homeland_security_book.html>.

_____. "Using 21st Century Technology to Defend the Homeland." Available from <http://www.whitehouse.gov/homeland/21st-technology.html>. Internet, Accessed 6 April 2002.

Campbell, Kurt M., and Michèle A. Flournoy. To Prevail: An American Strategy for the Campaign Against Terrorism. Washington, D.C.: Center for Strategic and International Studies (CSIS) Press, 2001.

Capps, Allan. Editor-in-Chief. Journal of Homeland Security. Available from <http://www.homelandsecurity.org/journal/>. Internet. Accessed 6 April 2002.

Cilluffo, Frank J. "Combating Terrorism: In Search of a National Strategy." Statement of Frank J. Cilluffo, Chairman, Committee on Combating Chemical, Biological, Radiological and Nuclear Terrorism, Homeland Defense Initiative, Center for Strategic and International Studies to the Subcommittee on National Security, Veterans Affairs and International Relations, U.S. House of Representatives Committee on Government Reform. Washington, D.C.: Center for Strategic and International Studies, July 2001.

_____. "Combating Terrorism: Options to Improve the Federal Response." Testimony of Frank J. Cilluffo, Chairman, Committee on Combating Chemical, Biological, Radiological and Nuclear Terrorism, Homeland Defense Initiative, Center for Strategic and International Studies to the U.S. House of Representatives Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management and the U.S. House of Representatives Committee on Government Reform Subcommittee on National Security, Veterans Affairs and International Relations. Washington, D.C.: Center for Strategic and International Studies, 24 April 2001.

_____. "Wired World: Cyber Security and the U.S. Economy." Testimony of Frank J. Cilluffo, Co-chairman, Cyber Threats Task Force, Homeland Defense Project, Center for Strategic

and International Studies to the Joint Economic Committee of the U.S. Congress. Washington, D.C.: Center for Strategic and International Studies, 21 June 2001.

Cilluffo, Frank J. Moderator. "Consequence Management Symposium." Co-sponsored by The Center for Strategic and International Studies (CSIS) and The U.S. Army War College Center for Strategic Leadership. Carlisle Barracks, PA, U.S. Army War College, 21 to 23 August 2001.

Cilluffo, Frank J, Joseph J. Collins, Arnaud de Borchgrave, Daniel Gouré, and Michael Horowitz. Defending America in the 21st Century: New Challenges, New Organizations, and New Policies. Executive Summary of Four CSIS Working Group Reports on Homeland Defense. Washington, D.C.: Center for Strategic and International Studies, December 2000.

Cilluffo, Frank J., Sharon L. Cardash, and Gordon N. Lederman. Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy. A Report of the CSIS Homeland Defense Project. Washington, D.C.: Center for Strategic and International Studies, May 2001.

Clapper, James R., Lt Gen (Ret), USAF. NIMA Statement of Strategic Intent. Washington, D.C.: National Imagery and Mapping Agency.

Clark, Timothy B. Editor. Government Executive Homeland Security Home Page. Available from <http://www.govexec.com/homeland/>. Internet. Accessed 6 April 2002.

Clinton, William J. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December 2000.

_____. A National Security Strategy for A New Century. Washington, D.C.: The White House, May 1997. The National Archives and Records Administration version of the Clinton White House homepage provided the electronic copy of the 1997 National Security Strategy located at <http://clinton2.nara.gov/WH/EOP/NSC/Strategy/>.

_____. A National Security Strategy for A New Century. Washington, D.C.: The White House, December 1999. The National Archives and Records Administration version of the Clinton White House homepage provides an electronic copy of the 1999 National Security Strategy at <http://Clinton4.nara.gov/media/pdf/nssr-1229.pdf>.

_____. A National Security Strategy of Engagement and Enlargement. Washington, D.C.: The White House, February 1996. The Federation of American Scientists homepage historical archive provided the electronic copy of the 1996 National Security Strategy located at <http://www.fas.org/spp/military/docops/national/1996stra.htm>.

Collins, Joseph J. and Michael Horowitz. Homeland Defense: A Strategic Approach. A Report of the CSIS Homeland Defense Project. Washington, D.C.: Center for Strategic and International Studies, December 2000.

Congressional Quarterly Special Report. "Homeland Security". Congressional Quarterly Daily Monitor. 7 February 2002. 1-20.

Crawley, Vince. "Shelton Departs, Citing Spy Force as Weak Link: Joint Chiefs Repeatedly Urged Congress to Boost Intelligence." Defense News, 1-7 October 2001, 6.

David, Ruth A. "Why is Homeland Security so Difficult?." Analytic Services Inc. (ANSER) Briefing Slides Presented to the Center for Strategic and International Studies. Washington, D.C.: ANSER, 21 December 2001.

Davis, M. Thomas. "Homeland Security: New Mission of a New Century." Analysis Center Papers. Washington, D.C.: Northrop Grumman, January 2002. Available from <http://www.capitol.northgrum.com/files/new_mission_new_century.pdf>. Accessed 6 April 2002.

de Borchgrave, Arnaud, Frank J. Cilluffo, Sharon L. Cardash, and Michèle M. Ledgerwood. Cyber Threats and Information Security: Meeting the 21st Century Challenge. A Report of the CSIS Homeland Defense Project. Washington, D.C.: Center for Strategic and International Studies, December 2000.

Defense News Special Report. "Homeland Security." Defense News. 28 October to 4 November, 33-52.

Department of Defense. Defense Science Board Task Force on Strategic Intelligence Needs for Homeland Defense. Washington, D.C.: Office of the Undersecretary of Defense For Acquisition, Technology, and Logistics, March 2001.

_____. Quadrennial Defense Review Report. Washington, D.C.: Department of Defense, 30 September 2001.

_____. Protecting the Homeland: Report of the Defense Science Board 2000 Summer Study, Executive Summary, Volume I. Washington, D.C.: Office of the Undersecretary of Defense For Acquisition, Technology, and Logistics, February 2001.

Department of the Army. Army Homeland Security (HLS) Strategic Planning Guidance. Washington, D.C.: Department of the Army, 10 September 2001.

_____. Intelligence and Electronic Warfare Operations. Field Manual 34-1 Washington, D.C.: U.S. Department of the Army, 27 September 1994. Available from <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-1/toc.htm>. Internet. Accessed 6 April 2002.

_____. "JCS Approved HLS Definitions." Briefing slide from the Army G-8 Deputy Chief of Staff for Programs. Washington, D.C.: Headquarters Department of the Army, 14 February 2002.

_____. U.S. Army Training and Doctrine Command (TRADOC), Supporting Homeland Defense. White Paper. Norfolk, Virginia: U. S. Department of the Army, May 1999.

Dickson, Don. Publisher. Homeland Defense Journal Home Page. Available from <http://www.homelanddefensejournal.com/>. Internet. Accessed 6 April 2002.

Fisk, Daniel W. "Top Priorities for Improving Intelligence and Law Enforcement Capabilities." A Report of the Working Group on Intelligence and Law Enforcement. In the Heritage

Foundation report Defending the American Homeland.53-74. Washington, D.C.: Heritage Foundation, 2002.

Frank, Diane. "Intell [sic] info-sharing net gains support." Federal Computer Week. 21 January 2001. Available from <http://www.fcw.com/fcw/articles/2002/0121/news-share-01-21-02.asp>. Internet. Accessed 6 April 2002.

____. "Intelink sees renewed interest." ." Federal Computer Week. 9 January 2001. Available from <http://www.fcw.com/fcw/articles/2002/0107/web-intelink-01-09-02.asp>. Internet. Accessed 6 April 2002.

Gouré, Daniel. Defense of the U.S. Homeland Against Strategic Attack. A Report of the CSIS Homeland Defense Project. Washington, D.C.: Center for Strategic and International Studies, December 2000.

Greenberg, Maurice R. and Richard N. Haas. Making Intelligence Smarter: The Future of U.S. Intelligence. Report of an Independent Task Force. New York: Council on Foreign Relations, 1996. Available from <http://www.fas.org/irp/cfr.html#views>. Internet. Accessed 6 April 2002.

Hirsch, Steve. "CIA performance disputed as Congress plans hearings." Government Executive Magazine. 1 April 2002. <http://www.govexec.com/news/index.cfm?mode=report&articleid=22605>. Internet. Accessed 6 April 2002.

Hughes, Patrick M. "A Case for Greater Support for the U.S. Intelligence Community." Journal of Homeland Security 20 January 2001. Available from <http://www.homelandsecurity.org/journal/Commentary/Hughes_Commentary.htm>. Internet. Accessed 6 April 2002.

____. "Helping The U.S. Intelligence Community Do Its Work." Washington Times, 10 February 2002.

Huntington, Samuel P. The Clash of Civilizations and the Remaking of World Order. New York: Touchstone, 1996.

Johnson, Loch K. Secret Agencies: U.S. Intelligence in a Hostile World. New Haven: Yale University Press, 1996.

Joint Chiefs of Staff. "Homeland Security Definitions." Briefing Slides of the J8 Planner Level Meeting. Washington, D.C.: Force Structure, Resources, and Assessment J8, Joint Staff, 28 November 2001.

____. Joint Doctrine for Intelligence Support to Operations. Joint Pub 2-0. Washington, D.C., Joint Chiefs of Staff, 9 March 2000. Available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf>. Internet. Accessed 6 April 2002.

____. U.S. Department of Defense Dictionary of Military Terms. New York: Arco Publishing, 1988.

Knott, Stephen F. Secret and Sanctioned: Covert Operations and The American Presidency. New York: Oxford University Press, 1996.

Larsen, Randy J. "A Primer on Homeland Security." Available from <http://www.homelandsecurity.org/bulletin/primer.htm>. Internet. Accessed 6 April 2002.

____. "An Initial Action Plan for the Office of Homeland Security: A follow-on to the 'Primer for Homeland Security." 7 November 2001. Available from <http://www.homelandsecurity.org/bulletin/ActionPlanforOfficeofHLS.htm>. Internet. Accessed 6 April 2002.

____. Director. Analytic Services, Inc. (ANSER) Institute for Homeland Security Home Page. Available from <http://www.homelandsecurity.org/>. Internet. Accessed 6 April 2002. ANSER operates the premier homeland security home page. So popular and precise, this essential home page posted a disclaimer in the wake of September 2001 to inform visitors that they were not the official White House homeland security home page.

Larsen, Randy J., Col (Ret), USAF and Dr. Ruth A. David. "Homeland Defense: Assumptions First, Strategy Second." Journal of Homeland Security. October 2000. Available from <http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=8>. Internet. Accessed 6 April 2002. Previously published in the Fall 2000 edition of Strategic Review.

Larson, Eric V. and John E. Peters. Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options. Santa Monica, CA.: Rand, 2001.

Lemley, Brad. "Internet 2: A Supercharged New Network with True Tele-Presence Puts the Needs of Science First." Discover, May 2002, 62-67.

Martin, Frederick Thomas. Top Secret Intranet: How the U.S. Intelligence Built INTELINK – The World's Largest, Most Secure Network. Charles F. Goldman Series on Open Information Management. Upper Saddle River, New Jersey: Prentice Hall, PTR, 1999.

Mathis III, Jeff W. Homeland Defense: What does it mean for the 21st Century. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 1 June 1999.

Miller, James A. Symposium Chairman. "The Intelligence Requirements of Homeland Security and the War on Terrorism: Essential Elements of Information, Techniques, and Tools." National Intelligence Symposium 2002." National Military Intelligence Association. Bolling Air Force Base, Washington, D.C., 12 and 13 March 2002.

Mitchell, Alison. "Ridge Is Opening a Center to Analyze Data." New York Times, 25 December 2001. The New York Times on the Web. Available from <http://www.nytimes.com/2001/12/25/national/25RIDG.html>. Internet. Accessed 3 April 2002.

Murdock, Clark. "Nature of the Campaign and Overarching Objectives." Unpublished Version 3 of Chapter 3 "The Imperative to Prevail and the Nature of the Campaign" in the Center for Strategic and International Studies collaborative effort To Prevail: An American Strategy for the Campaign Against Terrorism. n.p. October 2001.

National Commission on Terrorism. Countering the Changing Threat of International Terrorism. L. Paul Bremer III, Chairman. Washington, D.C.: National Commission on Terrorism, 2000. Available from <http://www.fas.org/irp/threat/commission.html>. Internet. Accessed 9 April 2002.

National Defense Panel. Transforming Defense: National Security in the 21st Century. Washington, D.C.: National Defense Panel, December 1997. Available from <http://www.fas.org/man/docs/ndp/front.htm>. Internet. Accessed 9 April 2002.

Newman, Patricia M. and James Player. Homeland Security: Report on the Workshops to Define a Framework for Action. Fort George G. Meade, MD: National Security Agency, January 2002.

Nuttle, David A. "Intelligence Turf Wars." Journal of Homeland Security 14 February 2002. Available from <http://www.homelandsecurity.org/journal/Commentary/nuttlecommentary.htm>. Internet. Accessed 6 April 2002.

Pincus, Walter. "Rumsfeld Casts Doubt On Intelligence Reform Changes Suggested by Presidential Panel." Washington Post, 9 April 2002, sec. 1A, p. 17.

Richelson, Jeffrey T. The U.S. Intelligence Community, 4th ed. Boulder: Westview Press, 1999.

_____. The Wizards of Langley: Inside the CIA's Directorate of Science and Technology. Boulder: Westview Press, 2001.

Seigle, Greg. "CIA, FBI developing intelligence supercomputer." Government Executive Magazine 12 February 2002. Available from <http://www.govexec.com/news/index.cfm?mode=report&articleid=22264>. Internet. Accessed 3 April 2002.

Shulsky, Abram N. Silent Warfare: Understanding the World of Intelligence, Second Edition, Revised by Gary Schmitt. Washington, D.C.: Brassey's (US), 1993.

Steele, Robert D. The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats. Carlisle, Pennsylvania: Strategic Studies Institute, February 2002.

Tennis, Patrick. Coordinator. "Army Homeland Security Workshop." Workshop. Fort Belvoir, Center for Army Analysis, 4 to 7 December 2001. LTC Patrick Tennis allowed the author to observe the Army War Plans homeland security requirements workshop.

Treverton, Gregory F. "Intelligence Crisis." Government Executive Magazine 1 November 2001. Available from <http://www.govexec.com/features/1101/1101s1.htm>. Internet. Accessed 6 April 2002.

Turner, Stansfield. Secrecy and Democracy: The CIA in Transition. Boston: Houghton Mifflin Company, 1985.

Tzu, Sun. The Art of War. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

U.S. Army War College. Communicative Arts Program Directive, AY02. Carlisle Barracks: U.S. Army War College, 2001.

U.S. Commission on National Security/21st Century. New World Coming: American Security in the 21st Century – The Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century. Gary Hart and Warren B. Rudman, Co-Chair. Arlington: U.S. Commission on National Security/21st Century, 1999. Available from <http://www.nssg.gov/Reports/NWC.pdf>. >. Internet. Accessed 9 April 2002.

_____. Road Map for National Security: Imperative for Change - The Phase III Report of the U.S. Commission on National Security/21st Century. Gary Hart and Warren B. Rudman, Co-Chair. Arlington: U.S. Commission on National Security/21st Century, 2001. Available from <http://www.nssg.gov/PhaseIIIFR.pdf>. Internet. Accessed 9 April 2002.

_____. Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom - The Phase II Report on a U.S. National Security Strategy for the 21st Century. Gary Hart and Warren B. Rudman, Co-Chair. Arlington: U.S. Commission on National Security/21st Century, 2000. Available from <http://www.nssg.gov/PhaseII.pdf>. Internet. Accessed 9 April 2002.

U.S. Intelligence Community. "U.S. Intelligence Community Home Page." Available from <http://www.odci.gov/ic/index.html>. Internet. Accessed 6 April 2002. From this home page the home pages of all 13 members of the Intelligence Community can be accessed.

Williams, James A., LTG (Ret), USA. Symposium Host. "Defense Intelligence Status 2001." National Military Intelligence Association. Fairfax, VA, 12 and 13 February 2002.